

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

Recommendation ITU-T Y.3001



ITU-T Y-SERIES RECOMMENDATIONS
**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-
GENERATION NETWORKS**

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3001

Future networks: Objectives and design goals

Summary

Recommendation ITU-T Y.3001 describes objectives and design goals for future networks (FNs). In order to differentiate FNs from existing networks, four objectives have been identified: service awareness, data awareness, environmental awareness, and social and economic awareness. In order to realize these objectives, twelve design goals have been identified: 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 falls approximately between 2015 and 2020. Appendix I describes technologies elaborated in recent research efforts that are likely to be used as an enabling technology for each design goal.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.3001	2011-05-20	13

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 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/>.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere.....	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	2
6 Introduction	3
7 Objectives	3
7.1 Service awareness.....	3
7.2 Data awareness	4
7.3 Environmental awareness.....	4
7.4 Social and economic awareness	4
8 Design goals	4
8.1 Service diversity	5
8.2 Functional flexibility	5
8.3 Virtualization of resources	6
8.4 Data access	6
8.5 Energy consumption.....	7
8.6 Service universalization.....	7
8.7 Economic incentives.....	8
8.8 Network management.....	8
8.9 Mobility	9
8.10 Optimization	9
8.11 Identification.....	10
8.12 Reliability and security.....	10
9 Target date and migration.....	11
Appendix I – Technologies for achieving the design goals.....	12
I.1 Network virtualization (virtualization of resources)	12
I.2 Data/content-oriented networking (data access)	12
I.3 Energy-saving of networks (energy consumption).....	13
I.4 In-system network management (network management).....	13
I.5 Network optimization (optimization)	14
I.6 Distributed mobile networking (mobility).....	16
Bibliography.....	17

Recommendation ITU-T Y.3001

Future networks: Objectives and design goals

1 Scope

This Recommendation describes objectives and design goals for future networks (FNs). The scope of this Recommendation covers:

- Fundamental issues to which insufficient attention was paid in designing current networks, and which are recommended to be the objectives of future networks (FNs)
- High-level capabilities and characteristics that are recommended to be supported by future networks (FNs)
- Target timeframe for future networks (FNs).

Ideas and research topics of future networks (FNs) that are important and may be relevant to future ITU-T standardization are included in Appendix I.

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.2205] Recommendation ITU-T Y.2205 (2011), *Next Generation Networks – Emergency telecommunications – Technical considerations*.
- [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 (2007), *Security Requirements for NGN release 1*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 identifier [ITU-T 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.

NOTE 1 – The plural form "Future Networks" (FNs) is used to show that there may be more than one network that fits the definition of a future network.

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

NOTE 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.

NOTE 4 – The word "difficult" does not preclude some current technologies from being used in future networks.

NOTE 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
OCDM	Optical Code Division Multiplexing
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", or "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 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] and [b-EC FI], and although 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 in the future. Nor is it known whether the growing market of new application areas will have the potential to finance the enormous investment required to change the networks, if the new architecture is to be sufficiently attentive 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 NWvirt], 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 are 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 handle 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" are not limited to specific data types like audio or video content, but describe 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 consumption of materials and energy and reduction of greenhouse gas emissions. FNs are recommended to also be designed and implemented so that 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 of 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 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, and reliability and security, may relate to multiple objectives. Figure 1 shows only the relationships between a design goal and its most relevant objective.

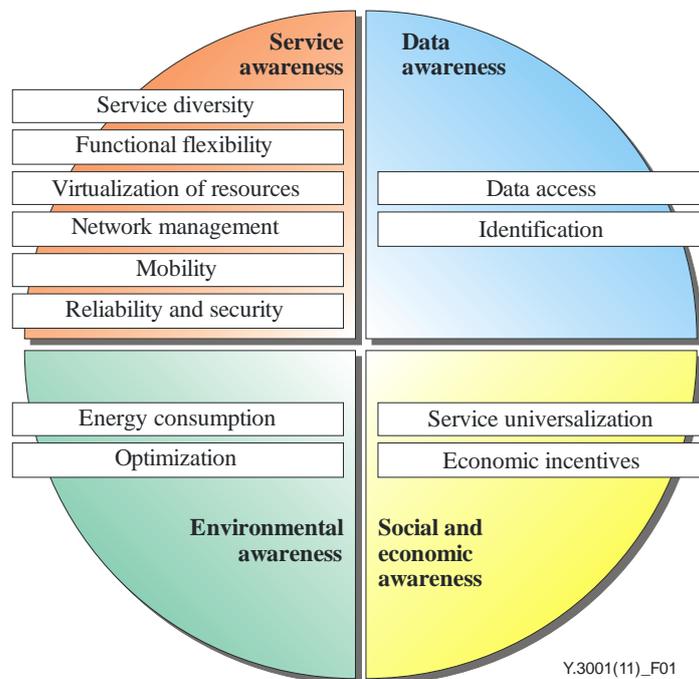


Figure 1 – Four objectives and twelve design goals of future networks

8.1 Service diversity

FNs are recommended to support diversified services accommodating a wide variety of traffic characteristics and behaviours. 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 and 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 Gbit/s, Terabit/s, 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 result 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 the 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 a very small bandwidth. On the other hand, there will be some high-end applications, such as high quality videoconference applications with high realistic sensation. Although the related terminal devices will not necessarily be very numerous, huge bandwidths will nevertheless 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 that keep pace with the rapid growth and change of user demands.

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 network design approach does not always 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 need to be carefully planned; otherwise, this may have an 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 transcoding 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 types of services in FNs. Services should coexist on a single network infrastructure without interfering with each other, in particular, when a network function is added or modified to support a certain service. FNs should 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 lessen obstacles to 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 among 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 network resources among virtual networks. Since multiple virtual networks can simultaneously coexist, different virtual networks can use different network technologies without interfering with each other, thereby 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 knowing their actual location. From a user standpoint, networks 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 accurate and correct data.

The amount and properties of digital data in networks are changing. Consumer-generated media are growing in an 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 to 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 depend mainly on the location of data, rather than the distribution of subscribers. Because of cloud computing, information and communication technology (ICT) resources, such as computing power and stored data in data centres, are increasing. Combined with the proliferation of mobile devices having insufficient ICT resources, this trend is shifting data processing from user terminals to data centres. FN designers therefore need to pay close attention to these changes, e.g., the growing importance of communications in data centres, and the huge number of transactions in and between data centres to fulfil user requests.

8.5 Energy consumption

FNs are recommended to use device-level, equipment-level, and network-level technologies to improve energy efficiency, and to satisfy customers' demands, with minimum traffic. FN device-level, equipment-level, and network-level technologies are recommended to not work independently, but rather to cooperate with each other in achieving a solution for network energy savings.

Rationale: The lifecycle of a product includes phases such as raw material production, manufacturing, use, and disposal, and all these phases 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 a day, as is often the case in networks. Among the various types of energy consumption, electric power consumption is usually predominant. 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. However, energy consumption and its resulting heat may become a significant physical limitation in the future, along with other physical limitations such as optical fibre capacity or operational frequency of electrical devices. These issues 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. However, this approach is facing difficulties such as high standby power and the physical limits of operational frequency. Therefore, not only device-level approaches, such as power reduction of electrical and optical devices, but also equipment-level 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-level, equipment-level, 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 competitive 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 a proper economic incentive.

Rationale: Many technologies have failed to be deployed, to flourish, or to be sustainable, because of inadequate, or inappropriate decisions, by the architect concerning intrinsic economic or social aspects, (e.g., contention among participants), or because of a lack of attention to surrounding conditions (e.g., competing technologies) or incentives (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. The IP layer did not provide a means to its upper layer to know if QoS was guaranteed from end-to-end. Initial IP network implementations also lacked proper economic incentives for the network providers to implement them. These are some of the reasons that have created obstacles to the introduction of QoS guarantee mechanisms and streaming services in IP networks, even when telecommunications ecosystem participants have tried to customize networks, or have asked others to provide customized networks, to start a new service and share its benefits.

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

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 to be a means of producing economic incentives in various fields, as the Internet grows and brings together diverse social functionalities. Different Internet participants often pursue conflicting interests, which has led to conflict over the Internet and controversy in international and 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, and to then efficiently and effectively transform these data into relevant information and knowledge for the operator.

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

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

The other problem is that current network operation and management systems largely depend on network operators' skills. A large difficulty exists therefore in how to make network management tasks easier and to inherit workers' knowledge. In the process of network management and operation, tasks that require human skill will remain, 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 transfer of knowledge and know-how between generations should also be considered.

8.9 Mobility

FNs are recommended to provide mobility that facilitates high-speed and large-scale networks 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 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 signalling functionalities regarding mobility are located at the core network. However, this approach may limit the operational efficiency because signalling 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 routes for application data and signalling data, should be supported for 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.

Technologies providing mobility services irrespective of a node's capability exist. However, this service is not easy when the node has limited capability, such as a 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 equipment.

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 a 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 user demand increases, the network equipment in the future will face various physical limitations, such as transmission capacity of optical fibre, operation frequency of electrical devices, etc.

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

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 use 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 re-emerges. 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) [ITU-T 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 so that they 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 challenges.

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 and authorization). This is an addition to existing security requirements, such as [ITU-T Y.2701]. This includes protecting the online identity and reputation, as well as providing users with the ability to control unsolicited communications. FNs should provide a 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; the 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 that 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 does not form an integral part of this Recommendation.)

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 the creation of logically isolated network partitions over a 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 NWvirt].

Users of logically isolated network partitions can programme 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 a 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 content distribution have been proposed. These include the 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] and [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 have been proposals where all data/contents have 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] and [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, see [b-NETINF] and [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 a variety of device-level, equipment-level, and network-level technologies [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 enable to achieve the same rate with less power using low-power devices/equipment, photonic switching, lightweight protocols, and so on [b-Baliga2007], and thus reduce the energy consumed per bit transmitted.
- 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 operations 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, redirecting, 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], and [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, empower 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. 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 worsen worse in the future due to the proliferation of different management systems caused by increasing services, so high-efficiency operations and management technologies are needed. Also, because current network operations and management depend mainly on the skills of the network manager, facilitating network management tasks and passing on 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 a sophisticated control interface and an inheritance system of operator knowledge and know-how 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] and [b-Nishikawa]
This provides the high-efficient operation and management to adapt all network systems that provide different services. The database technology is the key to automatically migrate old system data containing user and infrastructure information to the new system.
- b) Sophisticated control interface and inheritance system of operator knowledge and know-how [b-Kipler] and [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 fibre and states of communications, fault localization, and fibre 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 fibre, 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 hybrid optical/electrical layer, provides the minimum needed bandwidth for services and applications.

b) System-level optimization [b-Gunaratne]

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 optical code division multiplexing (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 fibre 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 in 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 signalling and data paths;
- enable the network administrator to control the signalling 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-ITU-T FG-FN Energy] ITU-T Focus Group on Future Networks FG-FN-OD-74 (2010), *Overview of Energy-Saving of Networks*, December.
- [b-ITU-T FG-FN NWvirt] ITU-T Focus Group on Future Networks FG-FN-OD-73 (2010), *Framework of Network Virtualization*, December.
- [b-Anderson] Anderson, T., Peterson, L., Shenker, S., and Turner, J. (2005), *Overcoming the Internet impasse through virtualization*, Computer, IEEE Computer Society, Vol. 38, No. 4, pp. 34-41.
- [b-Baliga2007] Baliga, J., *et al.* (2007), *Photonic Switching and the Energy Bottleneck*, Proc. IEEE Photonics in Switching, August.
- [b-Bohl] Bohl, O., Manouchehri, S., and Winand, U. (2007), *Mobile information systems for the private everyday life*, Mobile Information Systems, December.
- [b-CCNX] Project CCNx (Content-Centric Networking).
<<http://www.ccnx.org/>>
- [b-Chabarek] Chabarek, J., *et al.* (2008), *Power Awareness in Network Design and Routing*, in Proc. IEEE INFOCOM'08, April.
- [b-Chiba] Chiba, T., and Yokota H. (2009), *Efficient Route Optimization Methods for Femtocell-based All IP Networks*, WiMob'09, October.
- [b-Clark] Clark, D., Wroclawski, J., Sollins, K., and Braden, R. (2005), *Tussle in Cyberspace: Defining Tomorrow's Internet*, IEEE/ACM Transactions on Networking, Vol. 13, No. 3, June.
- [b-Dannewitz] Dannewitz, C. (2009), *NetInf: An Information-Centric Design for the Future Internet*, in Proc. 3rd GI/ITG KuVS Workshop on The Future Internet, May.
- [b-EC FI] European Commission, Information Society and Media Directorate-General (2009), *Future Internet 2020: Visions of an Industry Expert Group*, May.
<http://www.future-internet.eu/fileadmin/documents/reports/FI_Panel_Report_v3.1_Final.pdf>
- [b-Gunaratne] Gunaratne, C. *et al.* (2008), *Reducing the energy consumption of Ethernet with adaptive link rate (ALR)*, IEEE Trans. Computers, Vol. 57, No. 4, pp. 448-461, April.
- [b-Gupa] Gupta, M., and Singh, S. (2003), *Greening of the Internet*, Proc. ACM SIG-COMM'03, August.
- [b-HIP] IETF Host Identity Protocol (hipHIP) Working Group.
<<http://datatracker.ietf.org/wg/hip/>>
- [b-Iiyama] Iiyama, N., *et al.* (2010), *A Novel WDM-based Optical Access Network with High Energy Efficiency Using Elastic OLT*, in Proc. ONDM'2010, 2.2, February.
- [b-Jacobson] Jacobson, V., *et al.* (2009), *Networking Named Content*, CoNEXT 2009, Rome, December.

- [b-Kafle] Kafle, V. P., and Inoue, M. (2010), *HIMALIS: Heterogeneous Inclusion and Mobility Adaption through Locator ID Separation in New Generation Network*, IEICE Transactions on Communications, Vol. E93-B No. 3, pp.478-489, March.
- [b-Kimura] Kimura, H., *et al.* (2010), *A Dynamic Clock Operation Technique for Drastic Power Reduction in WDM-based Dynamic Optical Network Architecture*, in Proc. S07-3, World Telecommunication Congress (WTC).
- [b-Kipler] Kilper, D. C., *et al.* (2004), *Optical Performance Monitoring*, J. Lightwave Technol., Vol. 22, pp. 294-304.
- [b-Koponen] Koponen, T., Chawla, M., Chun, B., *et al.* (2007), *A data-oriented (and beyond) network architecture*, ACM SIGCOMM Computer Communication Review, Vol. 37, No. 4, pp. 181-192, October.
- [b-Kubo] Kubo, T., *et al.* (2010), *In-line monitoring technique with visible light form 1.3 μ m-band SHG module for optical access systems*, Optics Express, Vol. 18, No. 3.
- [b-LISP] IETF Locator/ID Separation Protocol (lispLISP) Working Group. <http://datatracker.ietf.org/wg/lisp/>
- [b-MANA] Galis, A., *et al.* (2008), *Management and Service-aware Networking Architectures (MANA) for Future Internet – Position Paper: System Functions, Capabilities and Requirements*, University of Twente, December.
- [b-NAMED DATA] Named Data Networking. <http://www.named-data.net/>
- [b-NETINF] Network of Information (NetInf). <http://www.netinf.org/>
- [b-NICT Vision] National Institute of Information and Communications Technology, Strategic Headquarters for New Generation Network R&D (2009), *Diversity & Inclusion: Networking the Future Vision and Technology Requirements for a New-generation Network*, February.
- [b-Nishikawa] Nishikawa, K., *et al.* (2009), *Scenario Editing Method for Automatic Client Manipulation System*, Asia-Pacific Network Operations and Management Symposium.
- [b-PSIRP] Publish-subscribe Internet Routing Paradigm (PSIRP). <http://www.psirp.org/>
- [b-Sarela] Särelä, M., Rinta-aho, T., and Tarkoma, S., *RTFM: Publish/Subscribe Internetworking Architecture*, ICT-Mobile Summit 2008 Conference Proceedings, Paul Cunningham and Miriam Cunningham (Eds), IIMC International Information Management Corporation.
- [b-TMF NGOSS] Tele Management Forum GB930, *The NGOSS approach to Business Solutions* (2005), Release 1.0.
- [b-UniverSELF] UniverSelf, realizing autonomies for Future Networks. <http://www.univerself-project.eu/>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems