International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

ITU-T Future Networks and Its Framework of Virtualization

Ziaul Ain Usmani[1], Dr. Gulabchand K. Gupta[2]
[1]*Research Scholar, JJT University, Jhunjhunu, Rajasthan, India*
[2]*Western College of Commerce and Business Management, Navi Mumbai, India*

***Abstract* — International Telecommunication Unioni-telecommunication (ITU-T) is an specialized agency in the field of information and communication technologies (ICTs) set up by the united nations. It is continuously making an effort to develop next generation and future network technologies such as network virtualization and published may Recommendations on it. ITU-T started working on the standardization of future networks in 2009 and published some initial recommendations. On network virtualization it has published Recommendation Y.3011. This article presents the background, objectives, design goals, and network virtualization which provides an important concept of logically isolated network partitions (LINP). ITU-T assumes that the target time frame for future networks (FNs) falls approximatelt between 2015 and 2020.**

***Keywords*—Future Network, ITU-T, Network virtualization, LINP, Recommendations of ITU-T.**

I. INTRODUCTION

ITU-T has published four important recommendations during 2009-2012. These are: Y.3001, Y.3011, Y.3021, and Y.3031 representing the first standard descriptions of future networks [1-4]. In addition to connectivity services, FNs are characterized by four objectives and twelve design goals. These design goals are advanced capabilities, features, and new network services that are needed together to realize FNs. It is believed that these recommendations will provide a sound foundation and appropriate guidance for subsequent FNs' realization, standardization, research, and development. In these recommendations, description of FNs is to meet assumption that trial services and phased deployment of future networks supporting the described objectives and design goals falls approximately between 2015 and 2020. This target date does not mean a network will change by that estimated time frame but that parts of a network are expected to evolve. Evolution and migration strategy may be employed to accommodate emerging and future network technologies. Such evolution and migration scenarios are topics for further studies.

There have been continuous efforts and progress regarding the research and development of future network technologies in recent years, such as network virtualization and software defined networking, automatic management, information centric networking (ICN), cloud networking, automatic management, and open connectivity. ITU-T started working on the standardization of Future network in late 2009, and it has developed some initial recommendation that lay out the essential directions for subsequent detailed work [1].

A future network (FN) is a network that is able to provide services, capabilities, and facilities that is difficult to be provided by the 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 which is operated as a single network. The plural form "Future Networks" (FNs) shows that there may be more than one network that fits the definition of a Future Network. A network of type b may also include networks of type a.

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 fair competition which reflect society's values remain important. At the same time, new requirements are emerging. Sustainability and environmental issues will be of vital important considerations over the long term. New areas of applications 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, by substantially reducing the production cost of equipments.

The basic architecture of large scale public networks is difficult to change because it contains enormous amount of resources needed to build it.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

Therefore, their architecture is carefully designed to be flexible enough to satisfy continually changing requirements. However, it is not known if the current networks can continue to fulfil changing requirements in the future. It is also not known whether the growing market of new application area will have the potential to fund the enormous investment required to change the networks. Research communities have been working on various architectures and supporting technologies such as network virtualization, energy saving of networks, and content-centric networks. Future networks trial services and phased deployment is estimated to fall approximately between 2015 and 2020. ITU-T Y.3001 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.

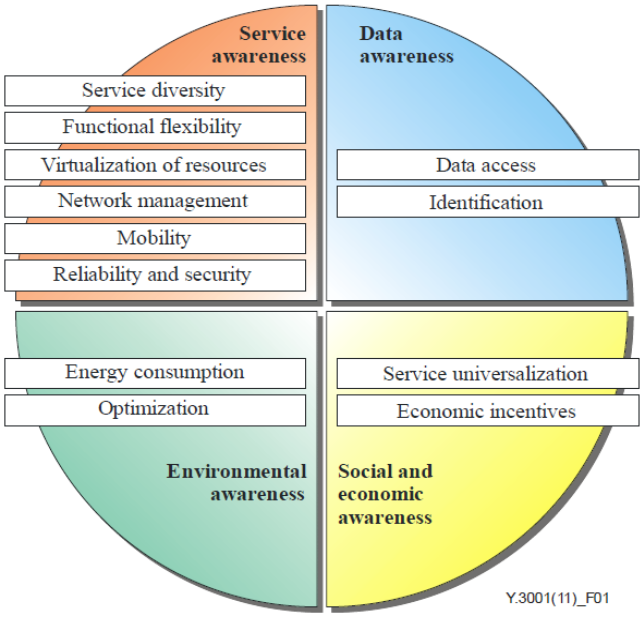
II. Objectives

FNs are recommended to fulfill the following objectives which reflect the new requirements that are emerging:

- *Service awareness:* FNs should provide services, without drastic increase in deployment and potential costs, whose functions are designed to be appropriate to the needs of applications and users.
- Data awareness: The FNs architecture should be optimized to handle the enormous amount of data in a distributed environment, and should enable users to access desired data safely, easily, quickly, and accurately, irrespective of their location.
- *Environmental awareness:* FNs should be environmentally friendly, should minimize their environmental impact such as consumption of materials and energy and reduction of greenhouse gas emissions, and should be designed and implemented so that they can be used to reduce the environmental impact of other sectors.
- *Social and economic awareness:* Considerations of social and economic issues should also be there in FNs so as to reduce the barriers to entry of the various factors involved in the network ecosystem. Development of FNs should 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.

III. Design Goals

FNs design goals are high-level capabilities and characteristics that should be supported by it. FNs support twelve design goals as illustrated in Figure 1 which also shows relationships between four objectives mentioned in section II above [5] [6].



The twelve design goals are:

- *Service diversity:* FNs should support diversified services accommodating a wide variety of traffic characteristics and behaviours. They should support a huge number and wide variety of communication objects, such as sensors and terminal devices, to achieve an all-encompassing communication environment.
- *Functional flexibility:* FNs are recommended to offer **functional flexibility** to support and sustain new services derived from user demands by enabling dynamic modifications of network functions in order to operate various network services that have specific demands. Current network design does not always provide sufficient flexibility.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

- *Virtualization resources:* FNs should support virtualization of resources associated with networks in order to support partitioning of resources so that a single resource could be shared concurrently among multiple virtual resources. It allows network to operate without interfering with the operation of the other virtual networks while sharing network resources among virtual networks.
- *Data access:* FNs should be designed and implemented for optimal and efficient handling of huge amount of data. They should have mechanism for promptly retrieving data regardless of their location. Because of importance of data access, FNs should provide users with the means to access appropriate data easily and without time-consuming procedures, while providing accurate and correct data.
- *Energy consumption:* FNs should use device-level, equipment-level, and network-level technologies, in cooperation with each other, to improve energy efficiency, and to satisfy customers' demands, with minimum traffic. Energy saving plays an important role in reducing the environmental impact of networks.
- *Service universalization:* FNs should enhance universalization of telecommunication services thus facilitating the development and deployment of networks and provision of services. They should facilitate and accelerate provision of facilities in differing area, such as towns or countryside, by reducing lifecycle costs of the network and.
- *Economic incentives:* Many technologies have failed to be deployed, to flourish or to be sustainable, because of inadequate decisions, or because of lack of attention to surrounding conditions or incentives. Thus ITU-T Y.3001 emphasises that FNs should consider social and economic issues such as the barrier to enter the market or the life cycle cost for the deployment and sustainability though it focuses on technical aspects.
- *Network management:* FNs should be able to efficiently operate, maintain and provide the increasing number of services and should be able to process massive amount of management data and information and then efficiently and effectively transform these data in to relevant information and knowledge for the operator.
- *Mobility:* Mobile networks are continuously evolving by incorporating new technologies thus are expected to include various heterogeneous networks. Thus FNs should 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 and should support mobile services irrespective of node mobility capability.
- *Optimization:* FNs should provide sufficient performance by optimizing network equipment capacity based on service requirement and user demand and should perform various optimizations within the network with consideration of various physical limitations of network equipment.
- *Identification:* FNs should provide a new identification structure that can effectively support mobility and data access in a scalable manner. Features such as mobility and data access require a provision for efficient and scalable identification [7] of a great number of network communication objects (hosts and data). IP addresses are host locators that depend on the points of attachment with the network. As the host moves, its identifier (ID) [8] changes, resulting in broken communication sessions Therefore, FNs 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.
- *Reliability and security:* FNs should operate and evolve with reliability and resilience in challenging conditions. They should be designed for safety and privacy of their users. They should also support any type of mission critical services, such as intelligence traffic management, smart grids, e-health, e-security, and emergency telecommunications with integrity and reliability.

IV. Target Date And Migration

The trial services and phased deployment of future networks supporting the objectives and goals as described above falls approximately between 2015 and 2020. Two factors decide the estimation:

The status of current and evolving technologies that would be employed in the experimentation and development of future networks;

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

Any novel development that might take place well beyond that estimated date is speculative.

The target date means that the parts of a network are expected to evolve, not necessarily the whole network. During these time frames, the evolution and migration strategies may be employed to accommodate emerging and future network technologies which are the topics of future studies.

V. ITU-T Future Network Framework Of Network Virtualization

Since realization of heterogeneous network architectures of multiple physical networks require huge costs on installation, operation and maintenance, therefore, a common physical network is required for future network to realize diverse services and heterogeneous network architectures. Since future and emerging network services require high-speed, large volume, low latency network connectivity for voice, video, and data base communications, it is necessary to ensure low power consumption by future networks. Future networks should also be more flexible and more reconfigurable so as to adapt to the changing requirements for future network services and applications.

To make diverse services flourish, the FNs should provide easy methods for experimenting and/or small scale deployment without causing unexpected effects for other networks, that is why it is often done by building completely separate networks. It will be an ideal environment to design, develop, and evaluate new services for developers, providers and the users of emerging technologies if experimental networks and/or test beds could be built on real networks that share common physical networks and could still provide isolated network environment.

These types of isolated and flexible networks are realized using network virtualization technology which supports a broad range of network architectures, services, and users that do not interfere with others. Thus, network virtualization is considered as a key technology for realizing future networks because it enables the easy establishment of experimental networks and accelerates research and development on future network technologies [2].

A. Network Virtualization Overview

A method that allows multiple virtual networks to coexist in a single physical network is called network virtualization. These multiple virtual networks are called logically isolated network partitions (LINPs). Physical resources are partitioned and abstracted as virtual resources. These virtual resources are interconnected to create a logically isolated network partitions (LINP) [9] [10] [11]. These virtual resources can be created on physical resources such as hosts, switches, and routers. Either virtual resources are allocated to each logically isolated network partition or multiple virtual resources are aggregated in to a single virtual source.

In an LINP network, virtual resources are separated from others and its capability can be reconfigured dynamically. It is a logical partition of the physical network having the same capability as that of physical network from which it is derived. It can also increase its capability by aggregating the multiple virtual resources. A user views the LINP as a network without network virtualization. A virtual resource is an abstraction of a physical or logical resource and its partition. It has the same mechanism as the physical or logical resource from which it is abstracted. Also, all the existing mechanism and tools for the physical or the logical resource from which it is abstracted can be inherited. In addition, a virtual resource has several interfaces to access and manage the virtual resources. Data plane interfaces, control plane interfaces, and management plane interfaces are typically included in these interfaces. [12].

Conceptual architecture of network virtualization is represented in Figure 1 [2]. This consists of LINPs over physical resources supporting network virtualization. Multiple virtual resources can share a single physical resource where each LINP consists of multiple virtual resources. An individual LINP manages each individual LINP. Physical resources in physical networks(s) are virtualized forming a virtual resource pool (Figure 1). Virtual resource manager (VRM) manages these virtual resources. The virtual resource manager interacts with the physical network manager(PNM) and performs control and management of virtual resources. Once virtual resources construct an LINP, an LINP manager is allocated to the LINP where the LINP manager performs a management function.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

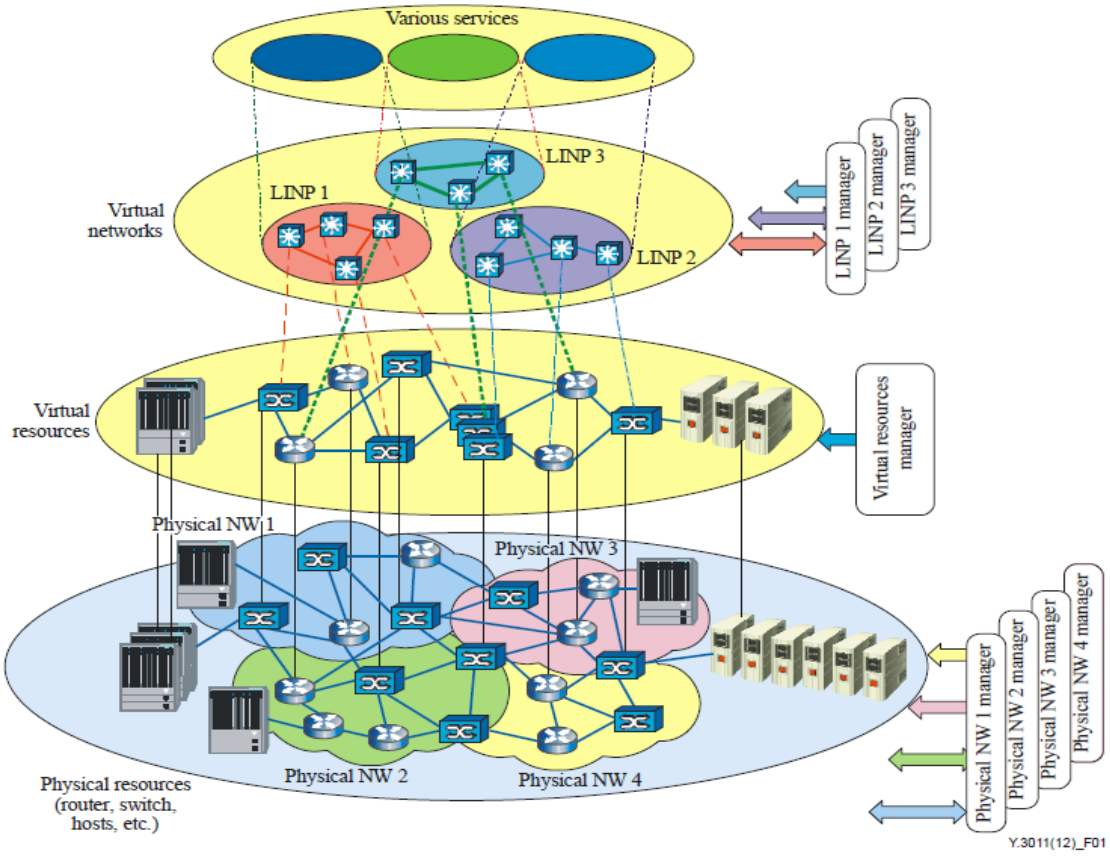


Figure 4.2.1 Conceptual architecture of network virtualization

The concept of LINP is represented in Figure 2 which consists of multiple coexisting LINPs over network resources supporting network virtualization. User requirements decide provision of each LINP.

Administration policy of VRM handles the requirement of LINPs. An LINP manager controls and manages each LINP. The VRM creates an LINP manager and allocates appropriate authorities to control each LINP.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

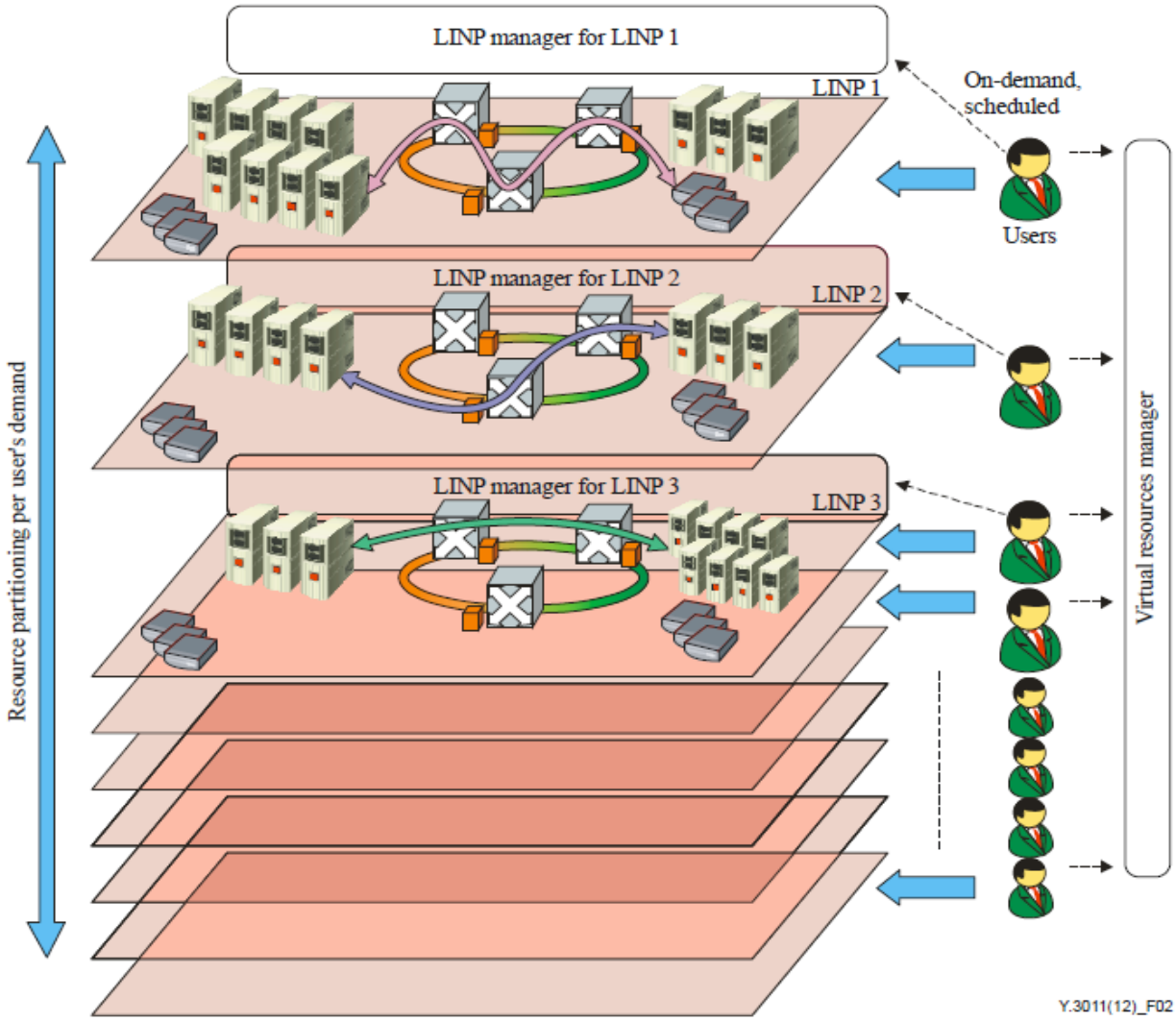


Figure 2 - Conceptual architecture of network virtualization.

An LINP has various characteristics as detailed below [12] [11]:

- *Partitioning:* Each LINP contains a set of resources which are independently manageable partition of physical resources. On a physical network, multiple LINP can coexist.
- *Abstraction:* A virtual resource can be abstracted directly from its physical resource and need not correspond directly from its physical resource so that other systems, applications or users access the capabilities of the virtual resource by using abstracted interfaces.
- These interfaces provide an efficient control of the virtual resource and guarantee compatibility for accessing the virtual resource. Interfaces can also be extended in order to provide increased capabilities. Through well defined and extensible interfaces, the virtual resources can be manipulated. These extensible interfaces can also be allocated to create, modify, reclaim, and release LINPs.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

- *Isolation:* All the virtual resources of one LINP are isolated from the other LINPs' virtual resources so that LINPs could not interfere with one another in terms of performance, security and namespace or any single LINP could disrupt other LINPs or physical networks. Also isolation prevents leak of data across LINPs.
- *Flexibility (Elasticity):* In order to maximize the usage of physical resources, LINPs' virtual resources are flexibly allocated, reclaimed, and released on demand. Flexibility also allows instantaneous and bursty usage as well as continuous usage of physical users.
- *Programmability:* LINPs' virtual resources can be programmed to develop, deploy and experiment with new communication protocols for innovative data dissemination and to facilitate efficient data processing to be enabled within the LINP.
- *Authentication, Authorization, and Accounting:* Usage of virtual resources which created an LINP must be authenticated and authorized to achieve safe and secure operations of LINPs. It prevents the abuse of the virtual resources and malicious attacks on them. To examine and monitor and to optimize the usage of virtual resources , it is necessary to account for the allocated virtual resources in physical networks.

In a nutshell, Utilization of physical resources can be improved by network virtualization by allowing multiple virtual resources to coexist in a physical resource. The abstraction and programmability also properly provides standard interfaces for managing and modifying the LINPs. It also gives a helping hand to support seamless modification and migration of the network so that it could provide services whose functions are designed to be appropriate to the needs of applications and users.

B. Problem spaces

Network virtualization can be used to mitigate the problems of current networks as discussed below:

- *Coexistence of Multiple Networks:* Conventional technology such as virtual private network (VPN) suffer from disadvantages in scalability, performance, and throughput so adding VPN mechanisms to existing protocols brings additional complexity and high data- processing costs [13]. It also suffers from considerable performance issues such as home agents and mobile nodes [14] [15]. Another conventional technology, virtual local area network (VLAN) suffers from scalability problems due to size of address space [16].

  By interconnecting virtual resources, network virtualization can provide LINPs where the interconnections may be realized by various mechanism not limited to conventional mechanism (such as VPN and VLAN) according to user and service requirements. Network virtualization can also provide secure isolation among LINPs from various points of views which includes security, performance or management, and support diversity of application, service management, network control, and architectures.
- *Simplified access to resources:* Heterogeneity of multiple heterogeneous physical resources could cause difficulty in accessing and managing the networks because of different types of access interfaces. Interoperability among various heterogeneous network resources is an important factor for future networks. Network virtualization allows the other systems, applications, or users to access the capabilities of resources by using abstracted interfaces [12]. These interfaces allow efficient access and control of virtual resources.
- *Flexibility in Provisioning:* Quick reconfiguration of LINPs is provided by network virtualization to enhance flexibility to environmental changes such as sudden traffic demand changes and network failures by dynamically changing their configurations. Network virtualization also allows adding additional logical resources to a virtual resource so that it could provide increased capability at lower cost than by adding physical resources.
- *Evolvability:* The disadvantage of building a separate physical test-bed is that the new technologies and services that have been successfully evaluated in the test-bed may not operate well in the real networks. Another disadvantage is the possibility of losing legacy support or backward compatibility. Network virtualization permits the network providers to integrate legacy support by allocating the existing networks to LINPs where the LINPs will ensure that the existing services and technologies can remain unchanged.

C. Design goals

Design goals of realizing network virtualization cover various aspects such as capabilities, characteristics and some challenging issues which are investigated below:

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

- *Isolation:* LINPs can cause instability due to interference with each other. Network virtualization can mitigate these problems by providing secure isolation, such as performance and security, among LINPs.
- *Network abstraction:* Hiding the underlying characteristics of network resources and establishing simplified interfaces for accessing the network resources (called network abstraction) allows the selective exposure of key network functionalities in networks by defining the abstraction level. It opens a new possibility to provide higher level interfaces thereby increasing the accessibility.
- *Topology awareness and quick reconfigurability:* During the construction of LINPs, network virtualization should support topology awareness so that the virtual resources can effectively interact with each other. During the operation, each LINP needs to adjust its capability according to the changes of requirements and, therefore, the reconfiguration should be quickly done in order to minimize service disruption. Thus, network virtualization should offer methods for easy and rapid creation of LINPs and should dynamically reconfigure them.
- *Performance:* Network virtualization adds additional virtualization layer which adds overhead and degrades system performance including higher CPU utilization and lower bandwidth, therefore, the performance of the LINPs may not be as good as that of non-virtualized network. The performance degradation of virtualized networks, therefore, should be minimized.
- *Programmability:* Users can customize protocols for forwarding or routing functions by equipping LINPs with programmable control plane and data plane. Programmability can support flexibility in the control plane for easy adaptation of new control schemes on LINPs and also in data plane to enable different kinds of data processing. Therefore, in order to provide flexibility and evolvability of networks using new control schemes and new data processing capabilities, network virtualization should support both control and data plane programmability.
- *Management:* Network virtualization should provide an integrated management system that can access both the information of physical resources and virtual resources to manage the network operations such as monitoring, fault detection, topology awareness, reconfiguration, resource discovery/allocation/ scheduling, and customized control.
- *Mobility:* Mobility is the ability of movement of virtual resources, including users and services which are composed of, for example, computing resources, system images, and applications across LINPs. Network virtualization should support mobility in order to fulfil the requirements of LINPs.
- *Wireless:* Wireless links should be virtualized. If two LINPs coexist on the same hardware for user, communication activities from one LINP should not affect any reception behavior on the other LINP. Coherence (when a transmitter of one LINP is active, all of the corresponding receivers and potential sources of interference should be simultaneously active on their appropriate channels of operation), and isolation (when a node belonging to one LINP is receiving some signal pertinent to the LINP, no transmitter of a different LINP within the communication range of the receiver should be active in the same or partially over-lapping channel) characteristics of the wireless links should be maintained [b-Mishra]. Therefore, scheduling methods for transmission activities across different LINPs should maintained [17].

D. *Applicability*

The key characteristics and the design goals of network virtualization will be catalytic factors for achieving the objectives and design goals of the future networks. The factors such as isolation of multiple LINPs, abstraction of network resources, , flexibility in configuring and providing LINPs,, and support of mobility and wireless virtualization can contribute in realizing the objectives and design goals of the FNs. Network virtualization also has several disadvantages as mentioned below:

- Performance degradation of LINPs,
- Scalability issues for the number of possible LINPs in a shared physical network, and
- Possibility of crashing whole LINPs due to the failure or security problems on LINP management systems.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 3, September 2014)

Thus, both advantages and disadvantages should be carefully considered from the initial stage before developing and deploying network virtualization to current networks.

E. Environmental considerations

By changing the overall architecture of networks through network virtualization, resource consumption and energy consumption is changed. Network virtualization also enables operators to develop multiple LINPs on a single physical network which reduces the necessary physical resources for constructing networks. For example, reduction in use of optical fibre or copper cable generally reduces energy consumption. Hardware utilization is improved by allowing more than one service to operate on the same piece of physical resource by network virtualization. This lowers the energy consumption because a single machine under high load generally consumes less energy than several lightly-loaded machines. Also, resource consolidation can be achieved by network virtualization which regroups underutilized devices which further reduces the energy consumption. The drawback of the network virtualization is that the structure of each node such as routers and switches become more complicated, which may cause increase in energy consumption.

F. Security considerations

Since virtual resources of LINPs are made available to the users, therefore, various securities need to be provided to the LINPs. Security and privacy problems related to public cloud computing services, as investigated by [b-Jansen] can be applied to the network virtualization. In order to mitigate potential security problems, the security and privacy issues such as security and privacy requirements of users, service providers using LINPs, and and LINP providers should be considered. Also, the security and privacy of data and applications that are implemented and deployed in LINPs should be regularly kept under monitoring.

VI. CONCLUSIONS

ITU-T has published four important recommendations during 2009-2012. These are: Y.3001, Y.3011, Y.3021, and Y.3031 representing the first standard descriptions of future networks. Objectives and design goals fir future networks (FNs) are described in Recommendation Y.3001. The four objectives has been identified as: service awareness, data awareness, social awareness, and economic awareness.

To achieve these objectives, twelve design goals have been identified as: service diversity, functional flexibility, virtualization of resources, data access, energy consumption, service universalization, economic incentives, network management, mobility, optimization, identification, reliability and security. The framework of network virtualization is described in Recommendation Y.3011. It presents its motivation and definition, and describes the concept of logically isolated network partition (LINP) that is provisioned by network virtualization. This Recommendation also discusses the problem spaces of network virtualization and investigates its design goals. Finally, this Recommendation discusses the applicability of network virtualization by summarizing its advantages and disadvantages. An appendix provides detailed use cases on various aspects of network virtualization, such as experimental network and mobility.

REFERENCES

[1] ITU-T Recommendation Y.3001 (2011), "Future networks: Objectives and design goals"..

[2] ITU-T Recommendation Y.3011 (2012), "Framework of network virtualization for future networks".

[3] ITU-T Recommendation Y.3021 (2012), "Future networks: Framework of energy saving for future networks"

[4] ITU-T Recommendation Y.3031 (2012), "Future networks:

[5] Matsubara D. et al., "Towards Future Networks: A Viewpoint from ITU-T", IEEE Commun. Mag., Vol 51, no. 3, March 2013, pp 112-118.

[6] Masturba D. et al., "open the Way to Future Networks-A Viewpoint Framaeworkfrom ITU-T", FIA 2013, LNCS 7858, pp. 27-38, link.springer .com.

[7] ITU-T recommendation F.851 (1995): Universal Personal Telecommunication (UPT)-services description (service Set 1).

[8] ITU-T recommendation Y.2091 (2011): Terms and definition for Next Generation Networks.

[9] Chaudhury N. M. and BautabaR. (2010), "A Survey of Network Virtualization", Computer Networks, Vol 54 (No. 5, April), pp. 862-876.

[10] GENI: Global Environment for Network Innovations GDD-06-08 (2006), GENI Design Principles. Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullende

[11] Nakao, A. (2010), "Network Virtualization as Foundation for Enabling New Network architecture and Applications", IEICE Transactions on Communications, Vol. E93-B (No. 3), pp.-454-457.

[12] Vermesan O. and Friess P. (2011), "Internet of Things-Global Technologies and Social Trends"' Aalborg, Denmark: River Publishers.

[13] Berger T. (2006), "Analysis of Current VPN Technologies", in Proc. Of the first Int. Conf. on availability, Reliability and security (ARES 06), IEEE Computer Society, (April), pp. 108-115.

[14] IETF RFC 4093 (2005), "Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateway".

[15] IETF RFC 5265 (2008), "Mobile IPv4 Traversal across IPSec-Based VPN Gateways.

[16] Yu M. et al. (2011), "A Survey of Virtual LAN Usage in Campus Networks", IEEE Commun. Mag., Vol 49, no. 7, July 2011, pp 98-103.

[17] Smith, G et al. (2007), "Wireless Virtualization on Commodity 802.11 hardware", in Proc. Of Second ACM Int. Workshop on Wireless Network testbed, experimental evaluation and characterization WinTECH '07, New York; ACM, pp. 75-82.