International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3011

(01/2012)

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

Next Generation Networks – Future networks

Framework of network virtualization for future networks

Recommendation ITU-T Y.3011

ITU-T

International
Telecommunication
Union

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.3011

Framework of network virtualization for future networks

Summary

Recommendation ITU-T Y.3011 describes the framework of network virtualization for future networks (FNs). 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.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.3011	2012-01-13	13

Table of Contents

Page

Introduction

Future networks (FNs) are networks that will be able to provide revolutionary services, capabilities, and facilities that are difficult to support using existing network technologies. One of the basic objectives of FNs is service awareness. The number and range of services are expected to explode in the future, and FNs need to adapt to the surge in the number of services [ITU-T Y.3001]. That surge in the number of services makes it difficult to satisfy the requirements of every service on a single network architecture. However, it is unrealistic to realize heterogeneous network architectures using multiple physical networks because of the installation, operation, and maintenance costs. FNs therefore need to realize diverse services and heterogeneous network architectures on a common physical network.

The future information and communication infrastructure is expected to support arbitrary kinds of social and economic activities. For example, while a proliferating number of network services are emerging and such services require high-speed, large-volume, low-latency network connectivity for voice, video, database communications, it is also imperative to ensure low-power consumption. A mixture of contradicting goals, including those described above, is to be resolved by the flexibly reconfigurable networks that accommodate multiple virtual networks with different capabilities. It is therefore crucial to make the networks more flexible and more reconfigurable so that they continuously and dynamically evolve to adapt to the changing requirements for future network services and applications. It is especially important to optimize the usage of the limited resources and maximize the number of users of the resources by quickly and dynamically adapting to environmental changes, for example, the emergency situations caused by natural disasters, through tailoring the amount and the quality of resources allocated for each virtual network and switching between multiple virtual networks with different capabilities.

At the same time, to make diverse services flourish, it is preferable for networks to provide easy methods for experimenting and/or small-scale deployment. This has to be done without causing unexpected effects for others, so it is often done by building completely separate networks. 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, it will give developers, providers, and users of the emerging technologies an ideal environment to design, develop, and evaluate new services.

Network virtualization is a technology that realizes isolated and flexible networks in order to support a broad range of network architectures, services, and users that do not interfere with others. It also enables the easy establishment of experimental networks and accelerates research and development on future network technologies. Therefore, network virtualization is considered as a key technology for realizing FNs.

This Recommendation provides the framework of network virtualization technology.

Recommendation ITU-T Y.3011

Framework of network virtualization for future networks

1 Scope

This Recommendation defines network virtualization and provides an overview of, and motivation for, network virtualization. It also describes problem spaces, design goals, and applicability of network virtualization.

Use cases for network virtualization are discussed in an appendix.

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

3 Definitions

3.1 Term defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 future network (FN) [ITU-T Y.3001]: A network able to provide services, capabilities, and facilities difficult to provide using existing network technologies.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 logical resource: An independently manageable partition of a physical resource, which inherits the same characteristics as the physical resource and whose capability is bound to the capability of the physical resource.

NOTE – "independently" means mutual exclusiveness among multiple partitions at the same level.

3.2.2 logically isolated network partition (LINP): A network that is composed of multiple virtual resources which is isolated from other LINPs.

NOTE – "logically isolated", which is the counter concept of "physically isolated", means mutual exclusiveness of the subjects (i.e., network partition, in this case), while the original subjects may be physically united/shared within the common physical constraints.

3.2.3 virtual resource: An abstraction of physical or logical resource, which may have different characteristics from the physical or logical resource and whose capability may be not bound to the capability of the physical or logical resource.

NOTE – "different characteristics" means simplification or extension of the resource characteristics. "different characteristics" allows the virtual resource to expose access or control methods different from the original physical or logical resource.

3.2.4 network virtualization: A technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider and appearing as a single resource.

NOTE – Refer to the note of the definition of LINP for "logically isolated".

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FN	Future Network
IPsec	Internet Protocol security
LINP	Logically Isolated Network Partition
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
PNM	Physical Network Manager
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRM	Virtual Resources Manager

5 Conventions

None.

6 Overview

Network virtualization is a method that allows multiple virtual networks, called logically isolated network partitions (LINPs), to coexist in a single physical network. In order to provide LINPs, physical resources are partitioned and abstracted as virtual resources and the virtual resources are interconnected to create an LINP [b-Chowdhury][b-GENI GDD0608][b-Nakao]. These virtual resources can be created on physical resources such as routers, switches and hosts. As such, virtual resources are either allocated to each LINP or else multiple virtual resources are aggregated into a single virtual resource.

LINPs are isolated from each other, and when combined with programmability in virtual resources, users of LINPs can program the virtual resources on the virtualization layer. In other words, each LINP can provide the corresponding users with services similar to those provided by traditional networks without network virtualization. The users of LINPs are not limited to the users of services or applications, but can include service providers. For example, a service provider can lease an LINP and can provide emerging services or technologies such as the cloud computing service. The service providers can realize the emerging services as if they own a dedicated physical network. In order to facilitate the deployment of network virtualization, it is necessary to provide control and management procedures such as creating, monitoring, and measuring the status of LINPs.

Figure 1 represents the conceptual architecture of network virtualization, which consists of LINPs over physical resources supporting network virtualization. A single physical resource can be shared among multiple virtual resources and each LINP consists of multiple virtual resources. Each LINP is managed by an individual LINP manager. In the figure, the physical resources in a physical network(s) are virtualized and may form a virtual resources pool. These virtual resources are managed by the virtual resources manager (VRM). The VRM interacts with the physical network manager (PNM) and performs control and management of virtual resources. Once an LINP is constructed by using the virtual resources, an LINP manager is allocated to the LINP. The LINP manager performs a management function.

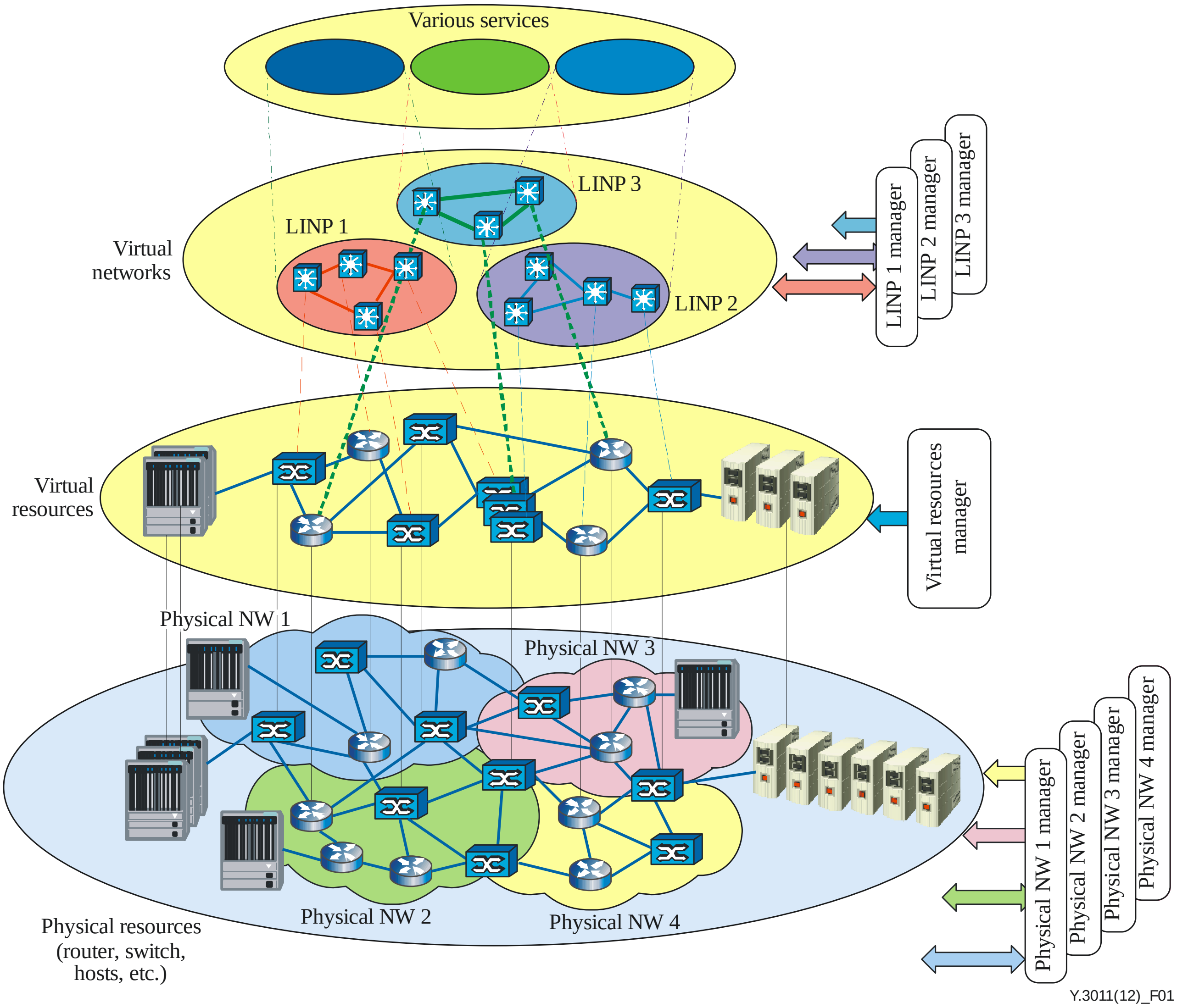


Figure 1 – Conceptual architecture of network virtualization

Figure 2 represents the concept of LINP, which consists of multiple coexisting LINPs over network resources supporting network virtualization. Each LINP is provided based on user requirements. The requirements are delivered to the VRM which coordinates the allocation of LINPs so that appropriate LINP is provided to users. The VRM handles the requirements based on its administration policy. Each LINP is controlled and managed by an LINP manager. The VRM which is controlling all virtual resources creates an LINP manager and allocates appropriate authorities to control each LINP. An LINP generated by using network virtualization has various characteristics, such as partitioning, isolation, abstraction, flexibility or elasticity, programmability, authentication, authorization, and accounting [b-Vermesan] [b-Nakao2]. The detailed description of the LINP characteristics is provided in Appendix I.

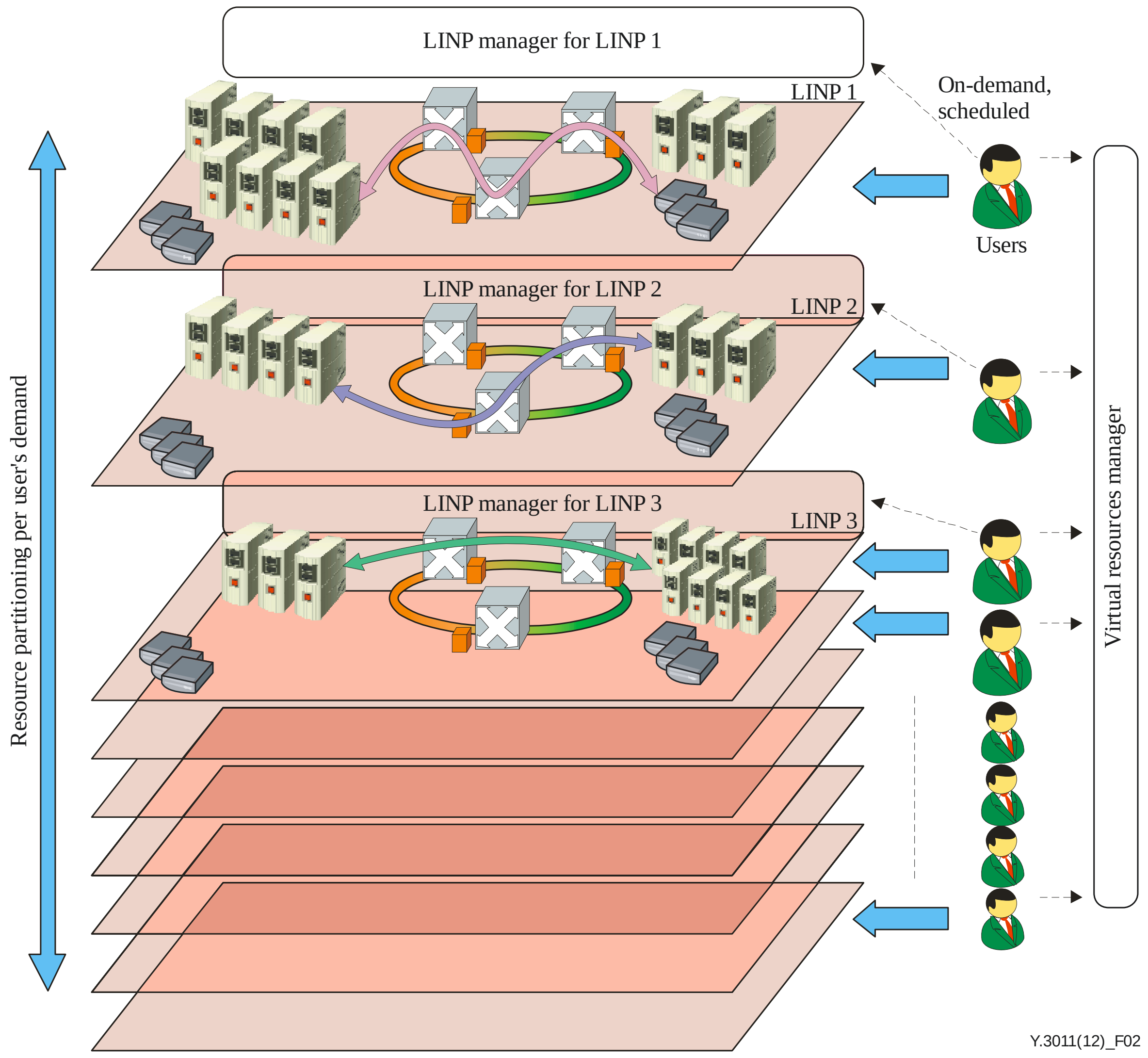


Figure 2 – Concept of LINP provided by network virtualization

Network virtualization can improve the utilization of physical resources by allowing multiple virtual resources to coexist in a physical resource. Also, the abstraction and programmability property provides standard interfaces for managing and modifying the LINPs and help to support seamless modification and migration of the network in order to provide services whose functions are designed to be appropriate to the needs of applications and users.

7 Problem spaces

This clause investigates the problems of current networks and how network virtualization can be used to mitigate the problems.

7.1 Coexistence of multiple networks

Conventional technologies, such as virtual private network (VPN) and virtual local area network (VLAN), are typically used for providing isolated networks over shared physical networks. However, it is known that these technologies have disadvantages and limitations.

For example, VPN relies on tunnelling mechanisms and internet protocol security (IPsec) in order to provide secure multiple networks over public networks. However, the current VPN technologies suffer from disadvantages in scalability, performance and throughput, which are caused by the complex encapsulation and authentication mechanisms. So, it appears that adding VPN mechanisms to existing protocols brings additional complexity and high data-processing costs such as a complex tunnel negotiation process in IPsec [b-Burger]. Furthermore, there are considerable performance issues on mobility-related network equipments such as home agents and mobile nodes [b-IETF RFC 4093] [b-IETFRFC 5265]. In the case of VLAN, the membership of VLAN should be determined prior to deploying VLAN, which requires static and complex manual configuration by the network administrator. Also, VLAN suffers from scalability problems due to the size of address space [b-Yu].

In addition, control of availability and performance and bandwidth guarantee for VPN and VLAN is difficult. If more users are operating on the networks, the bandwidth of the VPN tends to decrease and affect users of the entire system.

Network virtualization can provide LINPs by interconnecting virtual resources, but the interconnections may be realized by various mechanisms not limited to conventional mechanisms according to user and service requirements. Also, network virtualization can provide secure isolation among LINPs from various aspects, including security, performance or management, and support diversity of application, service, network control, management, and architectures.

7.2 Simplified access to resources

Networks typically consist of multiple heterogeneous physical resources such as routers and switches, but the heterogeneity causes a difficulty in accessing and managing the networks. In order to manage whole networks, network operators have to manage network resources with multiple types of equipment that may have different types of access interfaces. Also, FNs will contain not only the legacy components from networks, but also emerging new components from the development of up-to-date technologies. Thus, the interoperability among heterogeneous network resources will become important for FNs. For these reasons, access interfaces for different vendors have to be converged and managed on a common platform.

Network virtualization allows the abstraction of physical resources' characteristics so that other systems, applications, or users can access the capabilities of resources by using abstracted interfaces [b-Vermesan]. These interfaces can guarantee compatibility for accessing the virtual resources and provide an efficient control of the virtual resources.

7.3 Flexibility in provisioning

Flexibility refers to a capability of building a system, and expanding it as needed in order to adapt internal or external changes [b-Browne]. In legacy networks, it is difficult to rapidly provide networks appropriate for the requirements of various services because the provisioning of networks requires the actual deployment of physical resources. It is also difficult to adapt to the environmental changes such as sudden traffic demand changes and network failures by dynamically changing their configurations. Network virtualization provides quick reconfiguration of LINPs to enhance flexibility to environmental changes.

In legacy networks, the scale of a network is restricted by the number of physical resources, so scaling out, i.e., adding additional physical resources to the network, is one of the simple methods to increase scalability. However, this approach cannot be done in a flexible manner because adding physical resources implies not only hardware cost, but also maintenance and operations costs for floor space, operations, rack occupancy, etc. Also, if traffic demand is over-estimated in the network-design phase, existing networks will suffer from under-utilization.

Network virtualization allows the reuse of such resources, thereby achieving scalability and efficiency in the use of network resources. Network virtualization allows adding or aggregating additional logical resources to a virtual resource in order to provide increased capability at a lower cost than by adding physical resources.

7.4 Evolvability

If network providers want to deploy new network technologies and services or to migrate to a new network architecture, they need to build a separate test-bed so that the behaviour of the new technologies and services does not affect the current services. After evaluating the new technologies and services, network providers will deploy them to their networks in service.

However, this approach may have several disadvantages. First of all, experimental traffic of new network technologies and services needs to be tested in real networks and to coexist with user traffic because some issues, such as contention and policy enforcement, usually do not happen in the separate test-bed with small user traffic. Thus, the new technologies and services that have been successfully evaluated in the test-bed may not operate well in the real networks.

Therefore, researchers or developers of new network technologies and services may want to perform experimentation in the real networks rather than the test-bed. By doing so, when new technologies and services are accepted by users, they can be immediately put into service and the migration from the test-bed to real networks in service can be avoided.

Network virtualization can allow network provides to easily build logically separated test-beds by allocating securely isolated LINPs to the logically isolated test-beds for the experimental purpose.

The other disadvantage of building a separate physical test-bed is the possibility of losing legacy support or backward compatibility. Users may be reluctant to adapt new technologies because the new technologies may not support their existing services.

Network virtualization allows the network providers to integrate legacy support by allocating the existing networks to LINPs. The LINPs will ensure that the existing services and technologies can remain unchanged.

8 Design goals

This clause investigates the design goals of realizing network virtualization. These design goals cover various aspects such as capabilities, characteristics and some challenging issues.

8.1 Isolation

Since LINPs can be multiplexed over the physical network, such action is liable to cause instability due to interference with other LINPs. In order to mitigate these issues, in addition to conventional control plane and data plane isolation, network virtualization should provide secure isolations, such as performance and security, among LINPs.

For example, it is possible that a malfunctioning LINP consumes most of the physical resources, which decreases the performance of other LINPs due to network resource exhaustion.

Thus, network virtualization should provide the capability of regulating the upper limit of bandwidth usage by each LINP in order to maintain the overall throughput and performance.

Since LINPs created by network virtualization are isolated and independently managed, conventional security considerations for non-virtualized networks should be independently applied to each LINP too. In addition to that, a security problem of an LINP should not be spread to other LINPs.

8.2 Network abstraction

Network abstraction allows hiding the underlying characteristics of network resources from the way in which other network resources, applications, or users interact with the network resources, and establishing simplified interfaces for accessing the network resources. Network abstraction also allows selective exposure of key network functionalities in networks by defining the abstraction level. Network abstraction will open a new possibility to provide higher level interfaces, which increases the accessibility.

To support diverse network services, LINPs need to retain the capability of customizing network control and operations independent from those in the physical resources or other LINPs. At the same time, an LINP may want to avoid complex operations of physical resources that are dependent on the types of physical resources and equipment vendors.

Therefore, network virtualization should abstract the information of physical network resources and support the simplified or the higher level interfaces for resource control, in order to disengage the LINP from the complexity characteristic of the physical network resources.

8.3 Topology awareness and quick reconfigurability

Since network virtualization allows aggregation of virtual resources distributed in networks, it is necessary to discover these virtual resources. Furthermore, when constructing or reconfiguring an LINP, optimization may be required for effective use of the virtual resources. For example, for the users who want low end-to-end delay, topology awareness may help to provide low delay by using the shortest route, but still provide large bandwidth route for users who want large bandwidth and irrespective of delay.

Therefore, network virtualization should support topology awareness so that the virtual resources can effectively interact with each other during the construction of LINPs.

After creating LINPs based on users' requirements, the capabilities of LINPs need to be modified due to various reasons, for example the changes of users' requirements, the status of networks, policies of the virtual resources owners, and so on. Hence, each LINP needs to adjust its capability according to the changes of requirements and the reconfiguration should be quickly done in order to minimize service disruption.

Therefore, the network virtualization should offer methods for easy and rapid creation of LINPs and for dynamic reconfiguration of them.

8.4 Performance

Network virtualization is typically implemented by introducing a virtualization layer or an adaptation layer and the virtualization layer creates and manages LINPs. The virtualization layer is a layer between physical hardware and software running on a physical resource. This layer enables the creation of an isolated partition of the physical resource. Each partition is designed to accommodate different architectures and applications. The virtualization layer separates the hardware from the operating system environment. Network virtualization comes at a cost of reduced performance due to the virtualization layer. Network virtualization architecture includes an isolation partition with hardware device drivers, I/O stack and applications, placed over the virtualization layer that supports the control of physical hardware device controllers. This additional virtualization layer adds overhead and degrades system performance including higher CPU utilization and lower bandwidth. Thus, the performance of the LINPs may not be as good as the non-virtualized network.

Therefore, the performance degradation should be minimized.

8.5 Programmability

An LINP may be equipped with a programmable control plane and data plane so that users can use customized protocols, forwarding or routing functions in the LINP. In order to provide flexibility to the LINP, it is required to implement new control schemes on virtual resources. Programmability can support flexibility in the control plane and make it possible to easily adopt new control schemes on LINPs, and also in the data plane to enable various kinds of data processing.

In the control plane aspect, programmability involves control in LINPs such as routing, switching and monitoring for realizing proprietary control of traffic on an individual LINP. It also addresses parsing new communication protocols to be utilized in FNs. In the data plane aspect, it refers to data processing inside an LINP such as transcoding and data-caching for realizing new capabilities for data processing inside the network to enable innovative network services.

Therefore, network virtualization should support both control and data plane programmability in order to provide flexibility and evolvability of networks using new control schemes and new data processing capabilities. Also, each LINP should support the free deployment of control schemes or network architecture independent of other LINPs or physical networks.

8.6 Management

Each LINP can be a flexible aggregation of physical resources and virtual resources with appropriate network topology. From this perspective, a number of associations of not only physical-to-physical resources but also physical-to-virtual resources, and vice versa, have to be managed, which is not common in legacy network management. These complicated mappings cause difficulty in management, so visibility is required to understand all interconnections between physical and virtual resources over the physical networks.

Each LINP is isolated from others, so it has to be managed independently from others. At the same time, the management system for an LINP has to collaborate with the VRM. So, it is necessary to carefully define which part of management can be done by the LINP Manager, and how to align it with that of physical resources.

By considering the rapid changes of virtualized network environments, the visibility is essential for network management operations such as monitoring, fault detection, topology awareness, reconfiguration, resource discovery/allocation/scheduling, and customized control. One of the approaches for supporting management is to develop an integrated management system that may be implemented within the virtualization layer.

Therefore, network virtualization should provide an integrated management system that can access both the information of physical resources and virtual resources.

8.7 Mobility

Mobility in network virtualization is a movement of virtual resources, including users and services which are composed of e.g., computing resources, system images, and applications across LINPs. Each virtual resource can be moved according to users' demands and in order to retain the performance of LINPs. For example, users can be dynamically attached or reattached to one of the LINPs depending on the application characteristics. At the same time, to maintain the services' continuity for users, the services can also be moved together with the users without service downtime. In addition, the virtual resources can be added to improve network performance or removed for load balancing or energy-saving purposes.

To do that, it is essential that the virtual resource requirements from each LINP and users should be identified in advance or in a real time manner, and then these virtual resources should be moved to the corresponding LINPs in a limited amount of time. Since each LINP has different requirements, such as high network performance, low network latency, and energy efficiency, these requirements should be maintained in LINPs during an entire cycle of creation and termination of LINPs by supporting mobility in network virtualization. By doing so, flexible resource allocation to any LINP, real-time LINP maintenance and disaster-resistant network can be achieved.

Therefore, network virtualization should support mobility which is the ability of a movement of virtual resources in order to fulfil the requirements of LINPs.

8.8 Wireless

Wireless virtualization needs to consider some unique characteristics such as limited resource usage or signal interference that do not happen in wired networks. One of the biggest challenges in wireless virtualization is how to virtualize wireless links. Establishment of a wireless link requires the configuration of wireless channel parameters such as a channel of operation, appropriate setting of transmit power, or receiver sensitivity between a transmitter and a receiver. In order to provide two separate LINPs to users, communication activities from one LINP should not affect any reception behaviour on the other LINP if these two LINPs are to coexist on the same hardware.

However, the characteristics of wireless links can infer requirements such as coherence and isolation. Coherence means that when a transmitter of one LINP is active, all of the corresponding receivers and potential sources of interference as defined by the LINP should be simultaneously active on their appropriate channels of operation. Isolation means that 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 a partially-overlapping channel [b-Mishra].

Therefore, network virtualization should provide scheduling methods for transmission activities across different LINPs [b-Smith].

9 Applicability

In clauses 7 and 8, problem spaces and design goals for realizing network virtualization are investigated. This clause describes the applicability of network virtualization by summarizing its advantages and disadvantages.

As investigated in the previous clauses, it is expected that the key characteristics and the design goals of network virtualization will act as the catalyst to achieving the objectives and design goals of FNs. The isolation of multiple LINPs, abstraction of network resources, flexibility in configuring and providing LINPs, and support of mobility and wireless virtualization can contribute to their realization.

However, network virtualization also has several disadvantages, such as 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.

Therefore, before developing and deploying network virtualization to current networks, both the advantages and disadvantages should be carefully considered from the initial stage. Furthermore, some of the features of network virtualization should be selected according to the requirements of users and target services.

10 Environmental considerations

Network virtualization technology changes the resource (e.g., metal or fibre) consumption and energy consumption of networks by changing the overall architecture of networks.

This technology enables operators to develop multiple LINPs on a single physical network. This reduces necessary physical resources for constructing networks, e.g., optical fibre or copper cable, which generally reduces energy consumption.

This technology regroups a set of mechanisms allowing more than one service to operate on the same piece of physical resource, thus improving the hardware utilization. This opens the possibility to lower energy consumption because a single machine under high load generally consumes less energy than several lightly-loaded ones. Also, network virtualization can support resource consolidation which regroups underutilized devices to reduce the energy consumption.

A possible drawback is that the structure of each node, in particular the routers and switches, become more complicated, which may increase energy consumption.

11 Security considerations

Network virtualization enables on-demand provision and release of LINPs over configurable physical resources. Since LINPs consist of virtual resources that are made available to users, various security issues regarding network virtualization can be raised, especially for LINPs whose virtual resources are administered by an outside party that provides those LINPs to the users. Many key properties of network virtualization, such as flexibility, reconfigurability and network abstraction, make network virtualization one of the key technologies for FNs. However, those properties can cause unexpected security and privacy problems in traditional security models. [b-Jansen] investigates security and privacy issues related to public cloud computing services and some of the identified issues can also be applied to network virtualization. Therefore, the following security issues should be considered in order to mitigate potential security problems. Security and privacy issues should be considered during planning and designing network virtualization solutions. The issues can include security and privacy requirements of users, service providers using LINPs, and LINP providers. Also, it is necessary to keep monitoring the security and privacy of data and applications that are implemented and deployed in LINPs.

Appendix I

Detailed description of LINP

(This appendix does not form an integral part of this Recommendation.)

This appendix provides detailed description of the LINP that is discussed in clause 6.

An LINP is a network of virtual resources where the virtual resources are separated from others and its capabilities can be dynamically reconfigured. In other words, an LINP is a logical partition of the physical network and its capability is the same as, or subset of, the physical network. Also, the LINP can expand its capability by aggregating the multiple virtual resources. From the user's point of view, the LINP is treated as a network without network virtualization. A virtual resource is an abstraction of a physical or logical resource and its partition and has the same mechanisms as the physical or logical resource. It can also inherit all existing mechanisms and tools for the physical or the logical resource. In addition to the mechanisms above, a virtual resource has several interfaces to access and manage the virtual resource. These interfaces typically include data plane interfaces, control plane interfaces, and management plane interfaces [b-Vermesan].

An LINP generated by using network virtualization has the following characteristics:

(1) Partitioning

Each LINP consists of a set of virtual resources that are an independently manageable partition of physical resources. Multiple LINPs can exist on a physical network.

(2) Abstraction

A given virtual resource needs not correspond directly to its physical resource. The detailed information of the physical resource can be abstracted so that other systems, applications, or users access the capabilities of the virtual resource by using abstracted interfaces. These interfaces can be used to guarantee compatibility for accessing the virtual resource and provide an efficient control of the virtual resource. Also, it is possible to extend the interfaces in order to provide increased capabilities. The virtual resource can be manipulated through well-defined and extensible interfaces and allocated to create, modify, reclaim and release LINPs.

(3) Isolation

Virtual resources for forming an LINP are isolated from those for another so that LINPs may not mutually interfere with one another in terms of performance, security, and namespace and that any single LINP may not cause disruptions to other LINPs or physical networks. Data in one LINP do not leak across LINPs without authorization and applications can only communicate over configured network connections. Unauthorized accesses to other LINPs are prohibited.

(4) Flexibility (Elasticity)

Virtual resources for constructing an LINP are flexibly allocated, reclaimed and released on demand in order to maximize the accommodation of multiple LINPs on physical resources, to optimize the usage of the physical resources both temporally and spatially, and also to allow instantaneous and bursty usage as well as continuous usage of the physical resources.

(5) Programmability

Virtual resources for building an LINP can be programmed for developing, deploying and experimenting with new communication protocols for innovative data dissemination and for facilitating efficient data processing to be enabled within the LINP.

(6) Authentication, Authorization, and Accounting

Usage of virtual resources for creating an LINP must be authenticated and authorized so that it may achieve safe and secure operations of LINPs preventing the abuse of the virtual resources and malicious attacks on them. It is necessary to account for the allocated virtual resources in physical networks so that the integrity of virtual resources may be examined and monitored and the usage of the virtual resources may be optimized.

Appendix II

Use cases of network virtualization

(This appendix does not form an integral part of this Recommendation.)

In this appendix, the systematic knowledge of the use cases of network virtualization is described in order to clarify the purpose of network virtualization technology. The systematic description can be used as a guideline for describing the use cases, so further contributions regarding use cases should follow this guideline.

II.1 Case 1: Network virtualization for network service providers

II.1.1 Use case

– Overview

  - A network service provider often operates several different LINPs and provides different services on each LINP. By introducing network virtualization, the network service provider allows the construction and operation of a shared physical network accommodating multiple different services. Moreover, operators of each LINP are allowed to customize the configuration of their LINPs.

– Motivation

  - The operation of multiple networks which are physically independent and isolated often causes redundant network management tasks or unused physical resources to cope with an unexpected demand increase. Resource sharing by multiple services can solve such issues. However, existing technologies such as IP VPN and VLAN cannot provide hard isolation, programmability, quick reconfigurability, and topology-awareness. In the existing technology, users (e.g., service providers) are not allowed to obtain the information of a physical network topology and directly change virtual configurations such as IP routing and a virtual topology. Such controllability is effective in satisfying different service requirements.

– Usage

  - Network virtualization enables the creation of multiple LINPs over the shared physical network. Each LINP corresponds to a service network and is completely isolated from other LINPs. In addition, each LINP is reconfigurable and topology-aware. Such attributes enable service network operators to directly customize the configuration of their service network without the intervention of a physical network operator.

II.1.2 Current status of technology

A logical router technology has already been deployed in commercial IP routers. With this technology, multiple virtual routers can be created on a router. With programmable flow switching technology, the forwarding table of switch nodes can be controlled by the external servers. In the system level, network virtualization technologies are going to be deployed in commercial products.

As for network operation, [b-Masuda] constructed a network virtualization test-bed environment that consists of commercial IP routers and optical cross-connects, and also developed network management tools for managing multiple LINPs. They demonstrated on-demand LINP creation and the dynamic reconfiguration of an LINP. The operation of network virtualization is currently at an early stage of research development.

II.2 Case 2: Experiments on the feasibility of new network architectures [b-GENI GDD0608]

II.2.1 Use case

– Overview

- A test-bed network provides a part of its resources as an LINP to researchers developing new networking technologies. The researchers perform experiments to verify those technologies on the LINP.

– Motivation

- Verifying the feasibility of new network technologies in large-scale experimental networks or test-beds is vital to foster innovations in network architectures. Multiple user experiments can be performed concurrently on a single experimental network using network virtualization technologies. Existing test-bed networks do not allow users to customize network node function (e.g., protocols) or configurations (e.g., network topologies and forwarding tables). Researchers are able to fully customize the provided LINP and utilize the complete network environment as if the network is exclusively occupied by the user experiment. Thus, experiments over such a network will discover findings and observations that could not be obtained by emulation or simulation-based experiments.

– Usage

- Network virtualization allows multiple LINPs on the single test-bed network and each of the LINPs is fully programmable in terms of network architecture, control, and management, independently of other LINPs. Thus, researchers can perform experiments to demonstrate their new ideas efficiently and effectively by constructing their own LINP satisfying their experimental requirements.

II.2.2 Current status of technology

There are on-going network virtualization test-bed networks based on an open standard like OpenFlow [b-McKeown] and vendor-specific technologies like a logical router [b-JUNOS]. OpenFlow allows running of experimental protocols in programmable flow switches, while the logical router allows running of multiple IP protocol instances on a router.

II.3 Case 3: mobility in virtualized network

II.3.1 Use case

– Who?

- Network service provider (NSP) who provides network access by providing direct backbone access to the Internet.

– To whom?

- NSPs and end users

– Why?

- In order to provide continuous service and connection to the end users, an LINP requires support of the dynamic movement of virtual resources, services, and capabilities among the LINPs

– What?

- A change of the attachment point from one LINP to another by the end users calls for dynamic movement of each service and virtual resource of the LINP. From this perspective, flexible virtual resource allocation to any LINP, continuous and automatic optimization for LINPs and seamless movement, such as predictive LINP movement before underperforming networks or failures between LINPs, should be supported.

The use cases of mobility in LINPs are as follows:

Figure II.1 shows use cases of user and application mobility in LINPs.

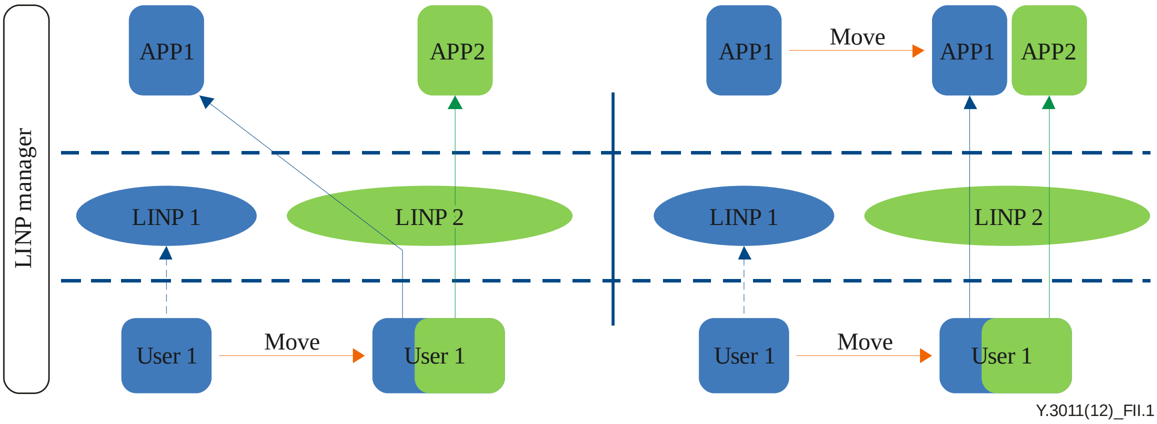


Figure II.1 – Use cases of user and application mobility

Each LINP may provide different virtual resources. In this example, LINP 1 is created based on low-powered virtual resources with very limited central processing unit (CPU) power and bandwidth. LINP 2 is created based on large virtual resources, which can provide large bandwidth and processing power. In this case, User 1 is currently connected with LINP 1 to use application APP1. When User 1 needs to use application APP 2 which requires high computing power, the LINP manager discovers LINP 2 for User 1. In addition, if User 1 still needs to use APP1, APP1 can be accessed from LINP 2 or APP1 can be moved from LINP 1 to LINP 2 for User 1. Therefore, the LINP manager will handle not only the user mobility but also the mobility of application, which is used by the user in the previous LINP.

Figure II.2 shows use cases of system image and resource mobility.

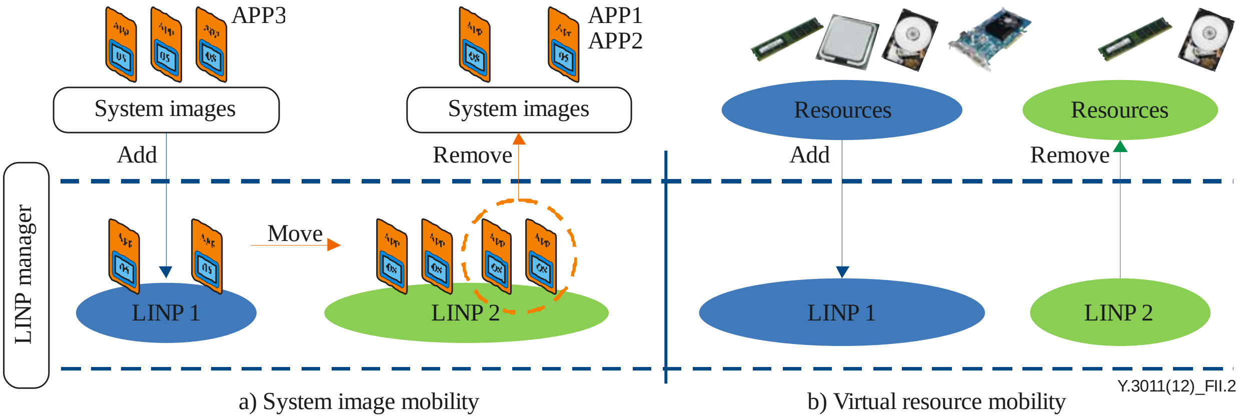


Figure II.2 – Use cases of system image and resource mobility

In this example, the system images can be moved without any interruption from LINP 1 to LINP 2 according to the user's demand, application type, and other reasons. Furthermore, both system images and resources can be added to LINP 1, and removed from LINP 2 in order to achieve high network performance and energy saving. Therefore, the LINP manager should handle the mobility of system images and resources between LINPs.

– When?

  - Network service provider requires these services now.

II.3.2 Current status of technology

There is a technology called live migration which allows a user to move a running virtual machine from one physical machine to another.

II.4 Case 4: Wireless access network virtualization

II.4.1 Use case

– Who?

  - Mobile network operator (MNO) who provides the end-to-end access and mobile services

– To whom?

  - Another MNO or a mobile virtual network operator (MVNO) who leases mobile network service from MNOs

– Why?

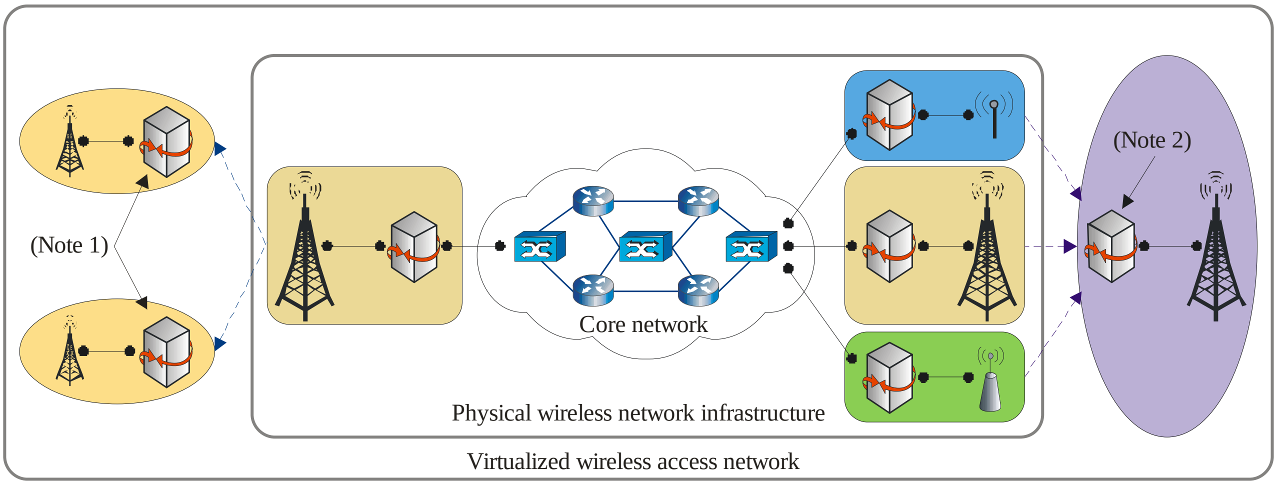
  - Future wireless networks will consist of multiple heterogeneous access technologies and each access technology has its own beneficial characteristics such as data rates, network capacity, coverage area and protocols as well. For these reasons, future wireless networks have a new challenge to provide the interworking and harmonization among heterogeneous networks.

– What?

  - Wireless network is also one of the resources in a virtualized network. Therefore, partitioning and aggregation, which are the applicability of network virtualization, should be reflected to the future wireless access networks.

The use cases of wireless access network virtualization are as follows:

Figure II.3 shows the use cases of partitioning and aggregation of wireless access network virtualization.


(Note 1)
(Note 2)
Core network
Physical wireless network infrastructure
Virtualized wireless access network
Y.3011(12)_FII.3

NOTE 1 – Use case 1: Partitioning of a single wireless network
NOTE 2 – Use case 2: Aggregation of different wireless networks

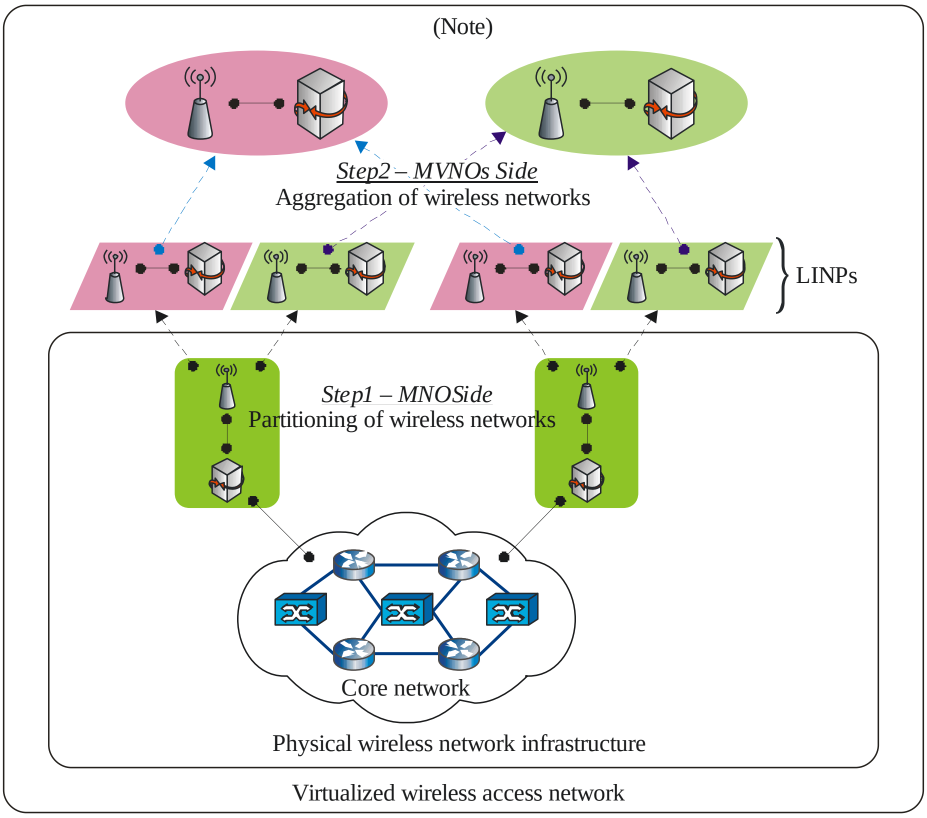
Figure II.3 – Use cases of partitioning and aggregation of wireless access network virtualization

The use case 1 in Figure II.3 depicts a use case of partitioning of a single wireless access network.

Explanation: by partitioning a wireless access network across multiple virtual networks, a single wireless access network can be used concurrently by multiple MVNOs for providing their own services and those virtualized wireless access networks are completely isolated from each other. Therefore, it provides an efficient use of existing physical wireless network infrastructure and facilitates deployment ease of new access networks for MVNOs.

The use case 2 in Figure II.3 depicts a use case of aggregation of different wireless networks.

Explanation: due to the coexistence of different wireless access networks, FNs are expected to be heterogeneous in nature. However, the problem is how to allocate the most suitable access network for the user when different access networks are available and it is closely relevant to network performance, cost and energy efficiency. In addition, another problem is how to reduce the disruption caused when users move frequently across different access networks. Since network virtualization allows the coexistence of different networks, the cooperation of different wireless access networks on demand by aggregating heterogeneous wireless access networks is possible. An example is that since each wireless access network provides service for a different coverage area, one wireless access network would cover the whole of the geographical service areas of other wireless access networks, or the service areas of heterogeneous wireless networks can be overlapped. In this case, multiple heterogeneous wireless access networks appear to the users as a single wireless network by aggregating different wireless access networks. Therefore, by aggregating wireless access networks, it can reduce stress on wireless networks which otherwise have to handle frequent movement of users. Furthermore, it is able to provide a consistently better user experience since wireless network connectivity for the users remains unaffected by user location or access network types. In other words, the user mobility is not handled within a virtualized wireless access network.


(Note)
Step2 – MVNOs Side
Aggregation of wireless networks
LINPs
Step1 – MNOSide
Partitioning of wireless networks
Core network
Physical wireless network infrastructure
Virtualized wireless access network

Y.3011(12)_FII.4

NOTE – Use case 3: Composite use case comprised of partitioning and aggregation of wireless networks

Figure II.4 – Composite use case of wireless access network virtualization

Figure II.4 shows a composite use case comprised of use cases 1 and 2 in Figure II.3.

Explanation: Each MVNO can lease a reasonable amount of wireless network resources from MNOs according to their own service requirements so that it can be realized by partitioning in network virtualization (Step 1 in Figure II.4). After that, a set of LINPs which is leased by the same MVNO can be aggregated (Step 2 in Figure II.4) into a single virtualized wireless network and thus the set of LINPs appears to the users as a single wireless network. This use case also has the same benefits as described above.

– When?

- Mobile network operator (MNO) requires these services now

II.4.2 Current status of technology

– There is a technology called wireless virtualization which describes how the radio resource sharing can be performed efficiently without interference between the different virtual wireless networks [b-Paul].

Bibliography

[b-IETF RFC 4093] IETF RFC 4093 (2005), *Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways.*

[b-IETF RFC 5265] IETF RFC 5265 (2008), *Mobile IPv4 Traversal across IPsec-Based VPN Gateways*.

[b-Browne] Browne, J. *et al*. (1984), *Classification of flexible manufacturing systems*, The FMS Magazine, (April), pp. 114-117.

[b-Burger] Berger, T (2006), *Analysis of current VPN technologies*. In: Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE Computer Society, (April), pp. 108-115, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1625300&isnumber=34117>.

[b-Chowdhury] Chowdhury, N.M. and Boutaba, R. (2010), *A Survey of Network Virtualization*, Computer Networks, Vol. 54 (No. 5, April), pp. 862-876.

[b-GENI GDD0608] GENI: Global Environment for Network Innovations GDD-06-08 (2006), *GENI Design Principles.*

[b-Jansen] Jansen, W. and Grance, T. (2011), *Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144*, (January).

[b-JUNOS] Juniper Networks, *JUNOS Software Routing Protocols Configuration Guide*, <http://www.juniper.net/>.

[b-Masuda] Masuda, A. *et al*. (2011), *Experiments of operating multiple virtual networks over IP-optical network*. In: Proceedings of the 37th edition of the European Conference on Optical Communication (ECOC 2011), Geneva, September 2011.

[b-McKeown] McKeown, N. *et al*. (2008), *OpenFlow: enabling innovation in campus networks*, *ACM SIGCOMM Computer Communication Review*, Vol. 38 (No. 2, April), pp. 69-74.

[b-Mishra] Mishra, A. *et al*. (2006), *Partially overlapped channels not considered harmful*. In: Proceedings of the Joint International Conference on Measurement and Modeling of Computer Systems, SIGMETRICS/Performance 2006, Saint Malo, France, June 2006, ACM.

[b-Nakao] Nakao, A. (2010), *Network Virtualization as Foundation for Enabling New Network Architectures and Applications, IEICE TRANSACTIONS on Communications*, Vol. E93-B (No. 3), pp.454-457.

[b-Nakao2] Nakao, A. *et al*. (2012), *Advanced Network Virtualization: Definition, Benefits, Applications, and Technical Challenges*, Network Virtualization Study Group (NVSG) White Paper (v.1.0, January), <http://nvlab.nakao-lab.org/nv-study-group-white-paper.v1.0.pdf>.

[b-Paul] Paul, S. and Seshan, S. (2006), *Technical document on wireless virtualization*, GENI: Global Environment for Network Innovations, Technical Report, (September).

[b-Smith] Smith, G. *et al*. (2007), *Wireless virtualization on commodity 802.11 hardware*. In: Proceedings of the second ACM international workshop on Wireless network testbeds, experimental evaluation and characterization WinTECH '07, Montreal, September 2007. New York: ACM, pp. 75-82.

[b-Vermesan] Vermesan, O. and Friess, P. (2011), *Internet of Things – Global Technological and Societal Trends*. Aalborg, Denmark: River Publishers.

[b-Yu] Yu, M. *et al*. (2011), *A Survey of Virtual LAN Usage in Campus Networks*, IEEE Communications Magazine, Vol. 49 (Issue 7, July), pp. 98-103.

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

Printed in Switzerland
Geneva, 2012