I n t e r n a t i o n a l   T e l e c o m m u n i c a t i o n   U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2320

(09/2015)

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

Next Generation Networks – Enhancements to NGN

Requirements for virtualization of control network entities in next generation network evolution

Recommendation ITU-T Y.2320

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
Enhancements to NGN	**Y.2300–Y.2399**
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based 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.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899

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

Recommendation ITU-T Y.2320

Requirements for virtualization of control network entities in next generation network evolution

Summary

Recommendation ITU-T Y.2320 provides requirements for virtualization of control network entities (VCN) in next generation network (NGN) evolution. The support of virtualization capabilities in NGN evolution – i.e., the application of virtualization techniques to NGN – enables a virtualized running environment (for control network entities) in NGN evolution.

The requirements provided in this Recommendation include the requirements of virtual infrastructures, virtualized network entities, and VCN management systems.

These requirements are built upon the virtualization scenarios provided in the appendix.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2320	2015-09-29	13	11.1002/1000/12583

Keywords

Control network entity, management, network entity, VCN, virtualization, virtualization of control network entities, virtual infrastructure, virtual machine , virtual machine monitor, VM, VMM.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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, i.e., 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/.

Table of Contents

Recommendation ITU-T Y.2320

Requirements for virtualization of control network entities in next generation network evolution

1 Scope

This Recommendation provides requirements for virtualization of control network entities (VCN) in NGN evolution. The support of virtualization capabilities in NGN evolution – i.e., the application of virtualization techniques to NGN – enables a virtualized running environment (for control network entities) in NGN evolution.

It is the common understanding that good performances can be achieved in network environments with virtualization of control network entities.

The requirements provided in this Recommendation include the requirements of virtual infrastructures, virtualized network entities, and VCN management systems. These requirements are built upon the virtualization scenarios provided in Appendix I.

Considerations concerning the virtualization of NGN entities are provided in Appendix II.

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.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 live migration: The process of moving a running virtual machine (VM) between different physical machines without interrupting the operating system and applications in the virtual machine.

NOTE – Central processing unit (CPU), memory, storage, and network connectivity of the virtual machine are transferred from the original physical machine to the destination machine.

3.2.2 virtualized control network entity (VCNE): A control network entity deployed on virtualized infrastructure (i.e., across one or multiple virtual machines (VMs)).

NOTE – A VCNE is composed of one or several components, and each component is hosted by a virtual machine (VM) which provides the virtualized computation environment running over the physical resources.

3.2.3 virtualized control network entity descriptor (VCNED): A configuration template that describes a virtualized control network entity (VCNE) in terms of its deployment and operational behaviour, and is used in the management of the lifecycle of a VCNE instance.

NOTE – Some examples of the VCNED information elements include:

- description of virtual resources;
- description of virtual machine (VM) configuration for the VMs pertaining to the VCNE;
- reference information of VM image(s);
- minimum and maximum number of VCNE instances which can be created to support scale out and scale in;
- VM initiation and termination workflow;
- connectivity of VMs for a specific VCNE in case multiple VMs are created.

3.2.4 virtualized control network entity package: An archive that includes a virtualized control network entity descriptor (VCNED), the virtual machine (VM) image(s) associated with the virtualized control network entity (VCNE), as well as additional artefacts.

NOTE – Artefacts can be used to check the integrity and to prove the validity of the archive.

3.2.5 virtual machine (VM): The virtualized computation environment that behaves like a physical server.

NOTE – A VM has all its ingredients (processor, memory, storage, and network) of a physical server and is generated by a virtual machine monitor (VMM). Virtual machines are capable of hosting a virtualized control network entity (VCNE) component.

3.2.6 virtual machine image: A file that can be interpreted by a virtual machine monitor (VMM) as a system hard disk drive.

NOTE – The operating system is pre-installed in the virtual machine (VM) image and, optionally, the control network entity software is pre-installed in the operating system.

3.2.7 virtual machine monitor (VMM): The software function that partitions the underlying physical resources and initiates virtual machines. It is also known as a hypervisor.

NOTE – This software may run either directly on top of the hardware (bare metal hypervisor) or on top of a hosting operating system (hosted hypervisor).

3.2.8 virtual machine template: A file that describes the hardware configuration of a virtual machine.

NOTE – The hardware configuration may describe the amount of CPU core, the number and speed of network interface cards (NICs), the size of the memory, the size of storage, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ATCA	Advanced Telecommunication Computing Architecture
CPCI	Compact Peripheral Component Interconnect
CPU	Central Processing Unit
FE	Functional Entity
NGN	Next Generation Network
NIC	Network Interface Card
P-CSC-FE	Proxy Call Session Control Functional Entity
S-CSC-FE	Serving Call Session Control Functional Entity
VCN	Virtualization of Control Network entities
VCNE	Virtualized Control Network Entity
VCNED	VCNE Descriptor

VM Virtual Machine

VMM Virtual Machine Monitor

5 Conventions

The following conventions apply in this Recommendation:

Affinity: This term is used to describe the relationship among different VMs, i.e., whether the different VMs are located in the same physical server or not, whether the different VMs are located in the same rack or not, etc.

Network entity: This term is intended as the practical, physical implementation of a single or a group of functional entities, as described in [ITU-T Y.2012], depending on the specific implementation and deployment policies.

6 Requirements of VCN in next generation network (NGN) evolution

The VCN system enables the VCN in NGN evolution.

NOTE 1 – Appendix II provides considerations concerning the virtualization of NGN entities.

Figure 1 shows the VCN system from a high level perspective: it includes the virtual infrastructure, the virtualized control network entities (VCNEs) running on the virtual infrastructure, and the VCN management system.

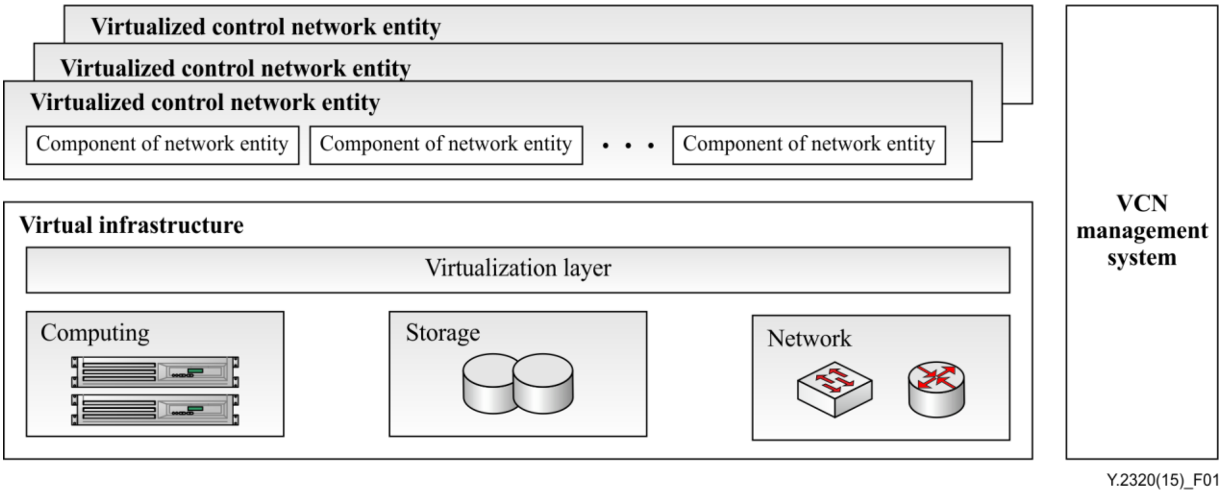

Figure 1 – Overview of the VCN system

The virtual infrastructure includes the hardware resources (computing, storage, and network resources) and the virtualization layer on top of them. The main functions of the virtualization layer are:

– abstraction of the hardware resources and decoupling of the software from the underlying hardware;

– allocation of virtual resources from hardware (physical) resources;

– provision of virtual resources to the VCNE software for VCNE to execute on.

NOTE 2 – The virtualization layer can be realized via a virtual machine monitor (VMM).

A virtualized control network entity (VCNE) consists of one or more components.

The VCN management system is used to support the virtualization capabilities of the VCN system (see scenarios in Appendix I). The VCN management system performs the management of the virtual infrastructure, including availability, allocation, release, fault, and performance management of virtualized resources, as well as fault, configuration, and performance management of physical facilities. It also performs the management of the virtualized control network entities, including lifecycle management of VCNEs such as VCNE on-boarding, instantiation, scaling and termination, as well as fault configuration and performance management of VCNE.

6.1 Virtual infrastructure related requirements

The virtual infrastructure is required to:

– support deployment of the VMs to physical server(s) according to the affinity policy defined in the VCNE descriptor (VCNED);

– support initiation and termination of VMs according to the virtual machine (VM) initiation and termination workflow defined in the VCNED;

– support resource usage monitoring for each of the VCNEs, every VM, and all physical servers;

– support live migration;

– provide shared storage for the VM images;

– support the automatic regeneration of VMs when active VMs crash;

NOTE – The crash of a VM may be caused by the crash of the host server, the related VMM, or the VM itself. When the crash is caused by the server or the VMM, the VCN system should support the VM regeneration on another server. When the crash is caused by the VM itself, the VM can be regenerated on the same server.

– be able to create or delete VMs;

– be able to adjust VM capacity (including computing, storage, and networking capacity).

6.2 VCNE related requirements

In order to support the capabilities provided by virtualization, the software implementation requires adequate design enhancements.

NOTE – The requirements of virtualized control network entities addressed in this Recommendation deal with the virtualization aspects of the control network entities, the aspects specific to each control network entity are out of the scope of this Recommendation.

a) VCNEs are required to support control network entity load monitoring and reporting to the management system.

b) The VCNEs are required to support high availability. The following is required:

   i) Failure of part of the related VMs does not affect any function of the control network entity.

   ii) Adding new VMs does not affect any function of the control network entity.

   iii) Adjusting VM capacity (including computing, storage, and networking capacity) does not affect any function of the control network entity.

6.3 VCN management system related requirements

The VCN management system is required to:

– be able to trigger scaling based on control network entity load or virtual infrastructure resource usage;

– support the on-boarding of VCNE packages;

NOTE 1 – The VM images in the package can contain the software of control network entities, or only contain the operating system.

– be able to use VCNED for management of the lifecycle of VCNE instances;

– support resource allocation for the virtualized control network entities according to their virtual resource requirements while the VCN system creates new virtualized control network entities;
– support resource recycling for the virtualized control network entities while, for example, the VCN system deletes existing virtualized control network entities, or removes VMs from virtualized control network entities, or reduces computing, storage, and networking capacity of VMs of virtualized control network entities, etc.;
– support prioritization of resource adjustment requests according to operation policy in order to manage potential resource adjustment conflicts;
– provide VM templates that satisfy different capacity requirements of different control network entities;
– perform the fault, configuration, and performance management of the physical facilities.

NOTE 2 – The VM templates may be pre-designed based on the configuration of physical facilities and the capacity requirements of different control network entities.

Appendix I

Scenarios concerning virtualization of control network entities in NGN evolution

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

NOTE – Figure 1 is a basis for all scenarios described in this appendix. Details are introduced in the various subclauses in order to describe the specific aspects of each scenario.

I.1 Auto-deployment of control network entity

Description

Auto-deploying a VCNE means creating its software instance. The software instance can be deployed onto a single VM or multiple VMs. A VCNE descriptor is used as the reference to modify or complement the parameters in a VCNE instantiation request. The operator can deploy the network entities by delivering the VM images remotely. It is not necessary for operators to deploy the hardware and maintain the network element on-site.

Pre-conditions

The construction of the VCN system has been completed and the VM images have been stored in the VM image database which can be viewed and selected by the operators; the VCNED has been uploaded onto a repository.

Operational flows

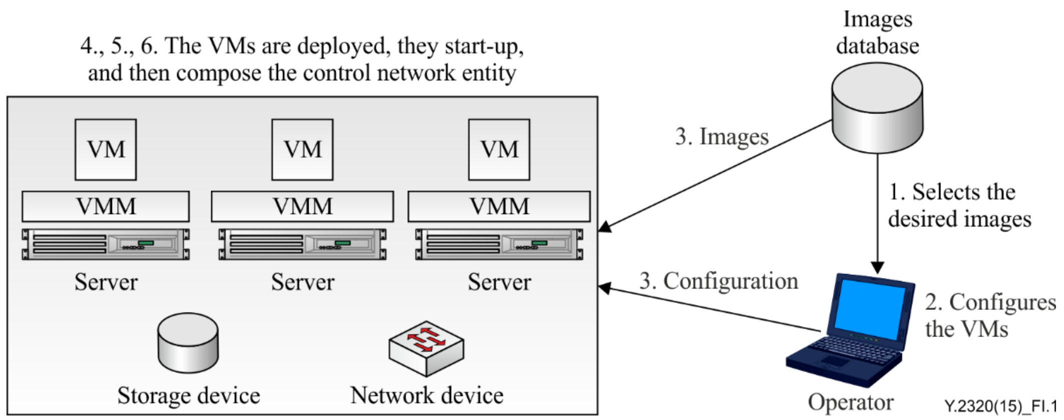

Figure I.1 – Control network entity deployment

1. According to the VCNED, the operator reserves the needed virtual resources for creating VMs and selects the desired VM images from the VM image database.
2. The operator configures the VMs based on the VCNED. The configuration may include the virtual hardware, the IP addresses, and the affinity among different VMs.
3. The images and the corresponding VM configurations are delivered to the virtual infrastructure.
4. The VMs are deployed to the physical servers, and the location of the VMs conforms to the pre-defined affinity policy.
5. The VMs start up. The configuration (including the IP address and the virtual hardware, etc.) conforms to the pre-defined parameters.
6. The virtual machines compose the control network entity.

NOTE – There are two options to construct the control network entity from the VMs.

Option one: The software of the control network entity has been set-up in each VM image. After the VMs start-up, the software of the control network entity runs immediately, and those VMs compose the network entity.

Option two: Only part of the software has been set up in one or more VM images (In most cases, the software is for the operation and maintenance to the control network entity, we can call it O&M sub-entity.), other VMs just run the operating system, those VMs will download the required software from the O&M sub-entity, set up the software, and then those VMs and the O&M VMs compose the control network entity.

I.2 Scaling

I.2.1 Scale out (automatic and on-demand)

Description

In a telecommunication network with virtualized control network entities, scale out (or scale horizontally) means to add more VMs to one VCNE, either automatically by the VCN system when the total VM usage or the service load service load exceeds the pre-configured upper threshold for this VCNE, or on-demand when the operator expects a VM usage or the service load increases for this VCNE. The following scenario uses VM as a trigger.

Pre-conditions

The control network entity (i.e., proxy call session control functional entity (P-CSC-FE)) has been deployed in the VCN system. There are multiple VMs constructing the control network entity, each VM runs a piece of software and increasing or decreasing the amount of VMs can increase or decrease the capacity of the network entity.

Operational flows

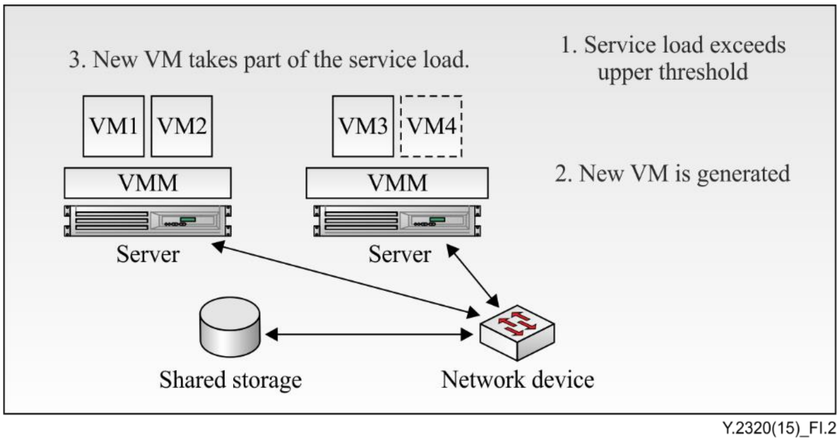

Figure I.2 – General procedure for scaling out

1. The VM usage or the service load exceeds the pre-configured upper threshold.
2. The VCN system detects that the threshold is reached and a new VM is generated in the VCN system. The new VM runs a piece of the network entity software.
3. The new VM takes part of the service load.

I.2.2 Scale in (automatic and on-demand)

Description

In a telecommunication network with virtualized control network entities, scale in means to remove existing VMs from one VCNE either automatically by the VCN system when the total VM usage or service load is below the pre-configured lower threshold for this control network entity, or on-demand when the operator expects a VM usage or service load decrease for this VCNE. The following scenario takes VM usage as example for the trigger.

Pre-conditions

The control network entity (i.e., P-CSC-FE) has been deployed in the VCN system. There are multiple VMs constructing the control network entity. Each VM runs a piece of software and increasing or decreasing the amount of VMs can increase or decrease the capacity of the network entity.

Operational flows

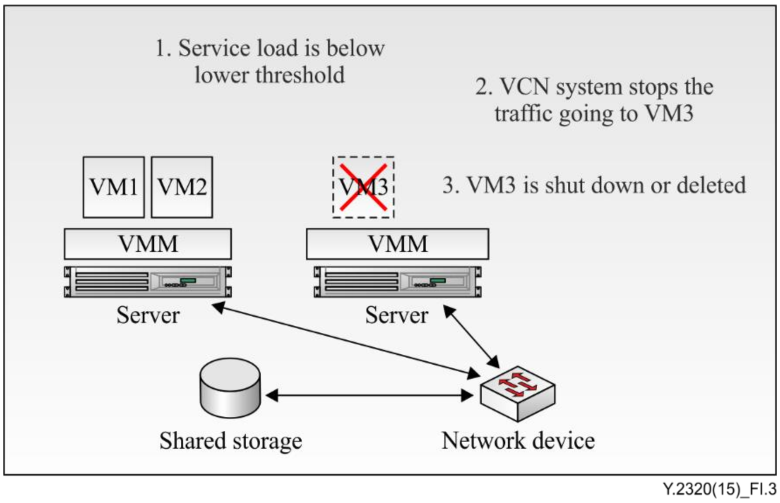

Figure I.3 – General procedure for scaling in

1. The VM usage or the service load is below the pre-configured lower threshold.
2. The VCN system detects the threshold is reached and it stops the traffic going to one of the VM (in this scenario, it is VM3).
3. When no traffic is handled by VM3, VM3 is shut down or deleted.

NOTE 1 – If there are no more VMs running on a given server, the server can be powered off by the VCN system.

NOTE 2 – Scaling includes scaling up and down; enhancing or reducing the configuration (i.e., computing, storage, and bandwidth) of VMs. Scaling up and down is not frequently used in the VCN.

I.3 Self-healing

NOTE – In this scenario, self-healing supports the service continuity when part of the computing, network, or storage devices stop.

Description

When VMs crash (the reason may come from the hardware, VMM or VM itself), the same VM can be re-constructed automatically and immediately. This feature can be used to ensure the high reliability of control network entities from the perspective of the VMs.

Pre-conditions

Pre-conditions are that the control network entity has been deployed in the VCN system; images of the control network entities (i.e., P-CSC-FE) are stored in a shared storage. There may be multiple VMs composing the control network entity. To ensure the reliability, the VCN system is designed in a way that if part of the VMs crash, it does not influence the service. For example:

- Two VMs form a pair, where one VM is the acting one which is the processing service, and another one is standing by. When the acting one crashes, the one which is standing by will take over the work and become the acting one.
- All the VMs form a pool, and they are all acting VMs. When part of the VMs crash, the running VMs will take over the work.

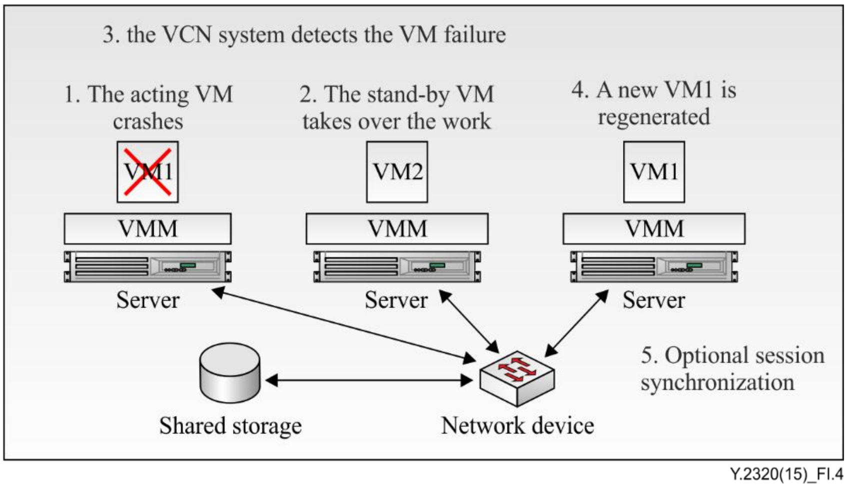

Figure I.4 – High reliability guaranteed by VM regeneration

The following flow, as seen in Figure I.4, illustrates the first example:

1. One of the acting VMs crashes.

   NOTE 1 – The crash may be caused by the failure of a physical server, VMM, or the VM itself.

2. The crash is detected and the stand-by VM takes over the work, becoming the acting VM.

   NOTE 2 –Crash detection, and take over by the stand-by VM are both application-level issues.

3. The VCN system also detects the failure of VM and regenerates the same VM immediately and automatically on another physical server.
4. The new VM starts up and works as the stand-by VM.
5. Optionally, if service continuity is required, the sessions running in VM2 and subsequent newly created sessions need to be synchronized to the stand-by VM.

I.4 Hardware change without interrupting the service

Description

When one physical server (i.e., server A) needs to be changed or upgraded, the VMs running on the server can be live-migrated to one or more other physical servers. In this scenario, using server B as an example, after all the VMs have been migrated to server B, server A can be changed or upgraded. The VMs are later be migrated back from server B to server A.

Pre-conditions

Pre-conditions are that one or more VMs of some control network entity are running on server A.

Operational flows

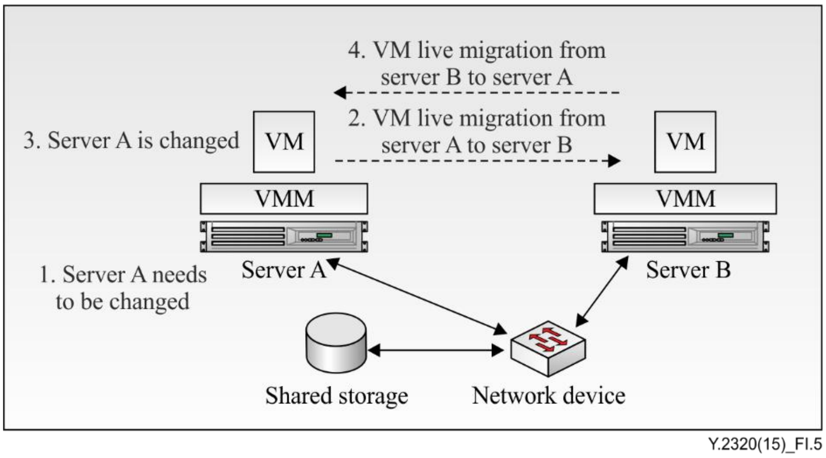

Figure I.5 – Hardware change without interrupting the service

1. Physical server A needs to be changed.
2. The VMs running on server A are live-migrated to server B.

   NOTE – VM live migration requires that the image of the VM is stored in a shared storage which can be accessed from the original server and the destination server.
3. Server A is changed.
4. The VMs are migrated back from server B.

I.5 Change of VCN system

Description

When the VMs of some network elements running on one kind of VCN system need to be moved to another VCN system, the VMs should be able to run on the new VCN system.

NOTE 1 – The VCN system includes the VMM and the management system of the VMM.

Pre-conditions

Pre-conditions are that the VMs of some network elements run on one kind of VCN system (i.e., VCN system 1).

Operational flows

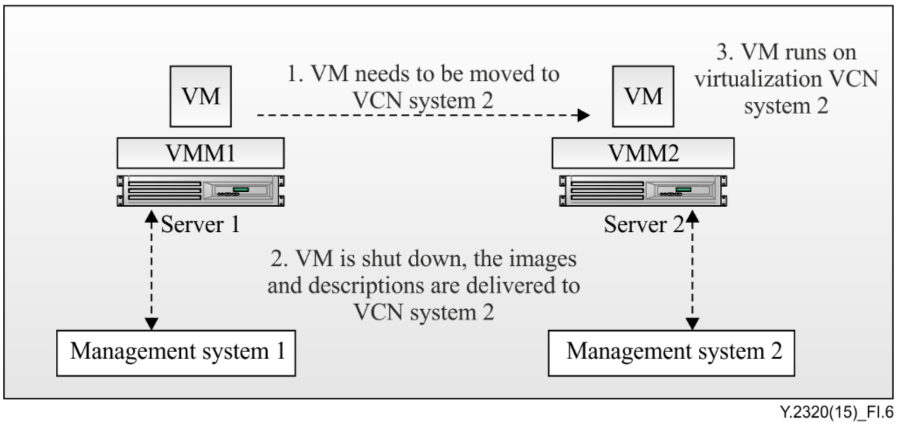

Figure I.6 – Change of VCN system

1. The VMs running on VCN system 1 need to be moved to VCN system 2.

   NOTE 2 –VCN system 1 is replaced by VCN system 2.

2. The VMs should be shut down and the image and description of the VMs should be delivered to VCN system 2 by the management system 2.

   NOTE 3 – Normally, live migration cannot be implemented between different VCN systems.

   NOTE 4 – The description of a VM includes the information of the VM, such as the virtual hardware configuration and the VM image.

3. The VMs run on VCN system 2.

I.6 Virtualized resource provision

Description

According to the service capacity requirements (i.e., supporting 1 million subscribers at 0.1 erl) and the configuration of the physical server (i.e., the computing speed of the central processing unit (CPU)), the VCN system can provide appropriate VM templates from which the user can choose. This mechanism can enhance the efficiency of the deployment of control network entities.

Pre-conditions

The pre-conditions are that the user needs to deploy a control network entity with certain capacity requirements (i.e., a serving call session control functional entity (S-CSC-FE) which supports 1 million users at 0.1 erl) and that the VCN system has stored some different VM templates that can satisfy different capacity requirements.

Operational flows

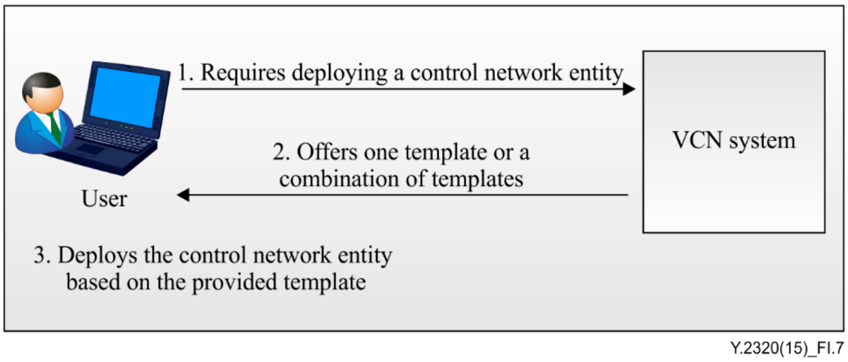

Figure I.7 – Virtualized resource provision

1. The user requires deploying a control network entity that should satisfy a given capacity.
2. The VCN system offers the most appropriate VM template (or a combination of different VM templates) which is able to satisfy the capacity requirements.

   NOTE – If neither of the single VM templates can satisfy the required capacity, a combination of different VM templates may be provided.

3. The user then deploys the control network entity based on the provided VM template.

Appendix II

Considerations concerning the virtualization of NGN entities

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

II.1 The virtualization technology provides benefits to the NGN

The NGN functional specifications have essentially focused on the NGN functional reference architecture, the capabilities of the different functional entities (FEs) and the reference points between those FEs.

The implementation aspects of the NGN (i.e., the hardware or the operating system) are out of the scope of the NGN functional specifications. From an implementation perspective, it has to be noted that the hardware infrastructure of the NGN functionalities is actually experiencing constant changes, from compact peripheral component interconnect (CPCI) devices or UNIX servers, to general purpose servers, such as advanced telecommunication computing architecture (ATCA) servers, and virtualization technologies have been introduced more and more.

The virtualization of network entities can bring various benefits, such as quick deployment, energy saving, hardware sharing, etc. In such a virtualization perspective, the NGN functional architecture needs to be enhanced, i.e., the way to manage and allocate virtual and physical resources needs to be designed, and the interactions between network entities and virtualization infrastructure need to be considered. Accordingly, the virtualization functions, including virtual infrastructure functions and management functions, become an integral part of NGN evolution.

II.2 The implementation of virtualized NGN entities requires enhancements

Virtualization does not imply modification of the functions of the NGN entities which are virtualized, such as session control of voice calls or mobility management. However, in order to support the capabilities provided by virtualization (i.e., adding or removing VMs in real-time), the software implementation of virtualized network entities requires adequate design enhancements. For example, the virtualized control network entities in a VCN system should support high availability, as well as enhanced load balancing and rebalancing capabilities (i.e., to adapt to VM changes, such as VM addition or removal for scaling).

II.3 Virtualized NGN control network entities will co-exist with non-virtualized NGN entities

Virtualized NGN control network entities won't replace the non-virtualized NGN entities when they are deployed. In most cases, the VCN systems will work in hybrid networks composed of both non-virtualized entities and virtualized entities, and the VCN systems will have to comply with the architecture and interfaces of non-virtualized infrastructure.

II.4 The virtualization of NGN entities starts from the control network entities

The VCN is the starting point for the support of virtualization capabilities in NGN evolution. It is commonly understood that good performance in network environments with VCNs can be achieved.

Bibliography

[b-ETSI GS NFV 001] ETSI GS NFV 001 V1.1.1 (Oct. 2013), *Network Functions Virtualisation (NFV); Use Cases*.

[b-ETSI GS NFV 003] ETSI GS NFV 003 V1.2.1 (Dec. 2014), *Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV*.

[b-ETSI GS NFV 004] ETSI GS NFV 004 V.1.1.1 (Oct. 2013), *Network Functions Virtualisation (NFV); Virtualisation Requirements*.

[b-ETSI GS NFV-MAN 001] ETSI GS NFV-MAN 001 V1.1.1 (Dec. 2014), *Network Functions Virtualisation (NFV); Management and Orchestration*.

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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, 2016