Document Number: DSP2034

Date: 2013-03-20

Version: 1.0.0a

Network Services Management Use Cases

Information for Work-in-Progress version:

IMPORTANT: This document is not a standard. It does not necessarily reflect the views of the DMTF or all of its members. Because this document is a Work in Progress, it may still change, perhaps profoundly. This document is available for public review and comment until the stated expiration date.

It expires on: 2013-07-15

Provide any comments through the DMTF Feedback Portal: http://www.dmtf.org/standards/feedback

Document Type: White Paper

Document Status: Work in Progress

Document Language: en-US

CONTENTS

Figures

Tables

Foreword

The *Network Services Management Use Cases* (DSP2034) contains macros that can be used when authoring DMTF documents. Use this macros template in conjunction with DSP1000_m.n.u, which contains instructions for how to use the template and the necessary boilerplate text.

Acknowledgments

The authors acknowledge the contributions from the members of the DMTF Network Services Management Work Group.   The following persons have been instrumental in the development of this white paper.

Editor(s):

- Khasnabish, Bhumip - ZTE Corporation
- Zhdankin, Aleksandr - Cisco

Contributors:

- Shah, Hemal – Broadcom
- Neely, Steven – Cisco
- Pardikar, Shishir – Citrix
- Parchem, John – Microsoft
- Lamers, Lawrence - VMware Inc.
- Ali, Ghazanfar - ZTE Corporation
- Chu, Junsheng - ZTE Corporation
- Hu, Jie - ZTE Corporation
- Khasnabish, Bhumip - ZTE Corporation
- Meng, Yu - ZTE Corporation
- Wang, Wei - ZTE Corporation

Introduction

Abstract

This document describes the problem of the network services management in virtualized and hybrid network environments and presents a set of network service-specific use cases applicable to such environments. The whitepaper discusses the applicability of the existing DMTF specifications, and identifies the target areas where the improvements of the existing or development of the new information models and management interfaces may be required.

Goals and Scope

Network Services Management (NSM) Work Group in DMTF is focused on the Network Services Profiles for the Routed Protocols (and routing protocols where needed) – IP (v4, v6) and layer-2 (or L2) connectivity as it relates to the services provided by the network infrastructure to the applications running in a cloud.

This white paper lists the use cases where these Network Service Profiles are needed, and provides analysis on how these Network Service Profiles will impact on the network models, including open virtualization format (OVF), Cloud Infrastructure Management Interface (CIMI), and Network Port Profile (NPP) XML Schema, currently defined by DMTF.

Network Services Management Use Cases

1 Scope

This document describes the problem of the network services management in virtualized and hybrid network environments. One of the objectives is to determine the features and functions of network infrastructure required to implement a set of high-priority network service-specific use cases applicable to such environments. The whitepaper also provides the analysis on applicability of the existing DMTF specifications, such as the OVF, CIMI, and NPP XML Schema. We achieve this by analyzing the gaps between the currently available OVF, CIMI, and NPP capabilities and the features and functions required from management models and interfaces. We then identify the target areas where the improvements of the existing or development of the new information models and management interfaces may be needed.

2 References

DMTF DSP2025, *Virtual Networking Management White Paper 1.0*
http://www.dmtf.org/standards/published_documents/DSP2025_1.0.pdf

DMTF DSP0263, *Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP 1.0*
http://www.dmtf.org/standards/published_documents/DSP0263_1.0.pdf

DMTF DSP0243, *Open Virtualization Format Specification 2.0*
http://www.dmtf.org/standards/published_documents/DSP0243_2.0.pdf

DMTF DSP2013, *CIM System Virtualization Model White Paper*
http://www.dmtf.org/sites/default/files/standards/documents/DSP2013_1.0.0.pdf

DMTF DSP2017, *Open Virtualization Format White Paper*
http://www.dmtf.org/sites/default/files/standards/documents/DSP2017_1.0.0.pdf

DMTF DSP8049, *Network Port Profile Schema Specification*
http://schemas.dmtf.org/ovf/networkportprofile/1/dsp8049_1.0.1.xsd

DMTF DSP2029, *Cloud Management for Communications Service Providers 1.0*
http://www.dmtf.org/sites/default/files/standards/documents/DSP2029%20_1.0.0a.pdf

DMTF DSP-IS0103, *Use Cases and Interactions for Managing Clouds*
http://www.dmtf.org/standards/published_documents/ DSP-IS0103_1.0.pdf

3 Terms and Definitions

In this section we define the terms that are used throughout this document. When applicable we use or update the definition from an existing DMTF specification.

3.1 Cloud

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (based on NIST definition, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).

3.2 Cloud Service

Cloud service is a service that utilizes shared computing, communications, and other resources over open or ubiquitous network based access to the resources (adapted from DSP-IS0103 and DSP2029).

3.3 Cloud Service Provider

Cloud Service provider is an organization that delivers cloud services to the Cloud Service Consumers, both internal and external (adapted from DSP-IS0103 and DSP2029).

3.4 Cloud Service Consumer or Cloud Consumer

Cloud service consumer is an entity that uses Cloud service from a Cloud Service Provider (adapted from DSP-IS0103 and DSP2029).

3.5 Cloud Consumer (or Cloud Service Consumer) Administrator

Cloud consumer Administrator is an entity that is responsible for administering the requests for resources and services from Cloud service consumer (based on information available in DSP-IS0103 and DSP2029).

3.6 Network

Network is a set of interconnected nodes capable of exchanging information.

3.7 Network Node

Network node is an addressable device in a network.

3.8 Network Policy

Network policy refers to a set of rules applied to the network. The rules are utilized for processing (security, quality of service, etc.) traffic.

3.9 Network Policy Enforcement Point

Identifies the entity where the Network Policies are applied

3.10 Network Policy Service

Network policy service enables application of network policies to various network components.

3.11 Network Policy Management Service

Network policy service enables management of network policies.

3.12 Network Policy Template

Network policy template is a set of Network Policy configuration parameters that can be used to create Network Policy instances.

3.13 Network Service

Network Service is a capability offered by a Service provider to its consumers that facilitates the transfer of the consumers’ information. Network service can be realized via virtual, physical or a combination of both types of network elements.

3.14 Network Service Template

Network Service template is a set of Network Service configuration parameters that can be used to create Network Service instances.

3.15 Network Topology Template

Network topology template is a topology configuration pattern that can be used to describe a network topology that can be instantiated.

3.16 Network Template

Network template is a combination of network service template and network topology template.

3.17 Virtual Machine

A virtual machine is a full encapsulation of the virtual hardware (including the CPU, controllers, Ethernet devices, and disks), virtual disks, and the metadata associated with it (adapted from DSP0243).

3.18 Virtual Computer System

A virtual system as applied to a computer system, e.g., a Virtual Machine, Hosted Computer, Child Partition, Logical Partition, Domain, Guest, and Container (DSP2013).

3.19 Virtual Desktop

Virtual desktop refers to delivery of the presentation of a desktop such as display, keyboard, mouse etc. on to another desktop or a thin client over a network.

3.20 Virtual Appliance

A virtual appliance is a set of pre-packaged virtual system(s) with guest operating system and applications (adapted from Section 1.2 of DSP2017).

3.21 Virtual Network Appliance

A virtual network appliance is a special type of virtual appliance that can be used for network connectivity and services, for example DNS, DHCP, load balancer, firewall, etc. or combination thereof.

3.22 Virtual System

A system that can be managed as described in DSP1042.

3.23 Virtual System Collection

A virtual system collection is a group of virtual systems related to each other in some manner.

3.24 Virtualized Network Entity

A virtualized network entity is an entity that facilitates creation or maintenance of a virtualized network.

4 Overview of Virtualized Networking

This section presents an overview of the virtualized networking concepts and principles.

4.1 Challenges of Virtualized Networking

In modern Data Centers, multiple network and service elements like Firewalls, Routers, AAA servers, DNS, QoS managers, Load balancers, etc. exist in LAN and SAN, which can be used to provide advanced network services. These elements may be implemented as virtual appliances as well as traditional dedicated devices and applications. In order to provide the unified management access to such network and service elements we are introducing the concept of Virtualized Networking, where we are looking at the externally manageable functionality of such entities abstracted from their actual realization.

NSM WG is focusing on developing specifications that help present a unified management view of the virtualized networking, services and their components to both Cloud service consumers and Cloud service providers.

Several challenging network related problems exist in virtualized networking environment:

- Configuration for network topology and network service deployment.
- Configuration for physical network hosting in virtualized networking environment.
- Rapid adaptation of network configuration for network service deployment.
- Network-Aware Hosting of content-aware applications such as Virtual Desktop (VD).

4.2 Virtualized Networking Components

Figure 1 shows a high-level schematic for abstraction of the network elements in order to expose them as the virtualized network entities (vNEs) for management.

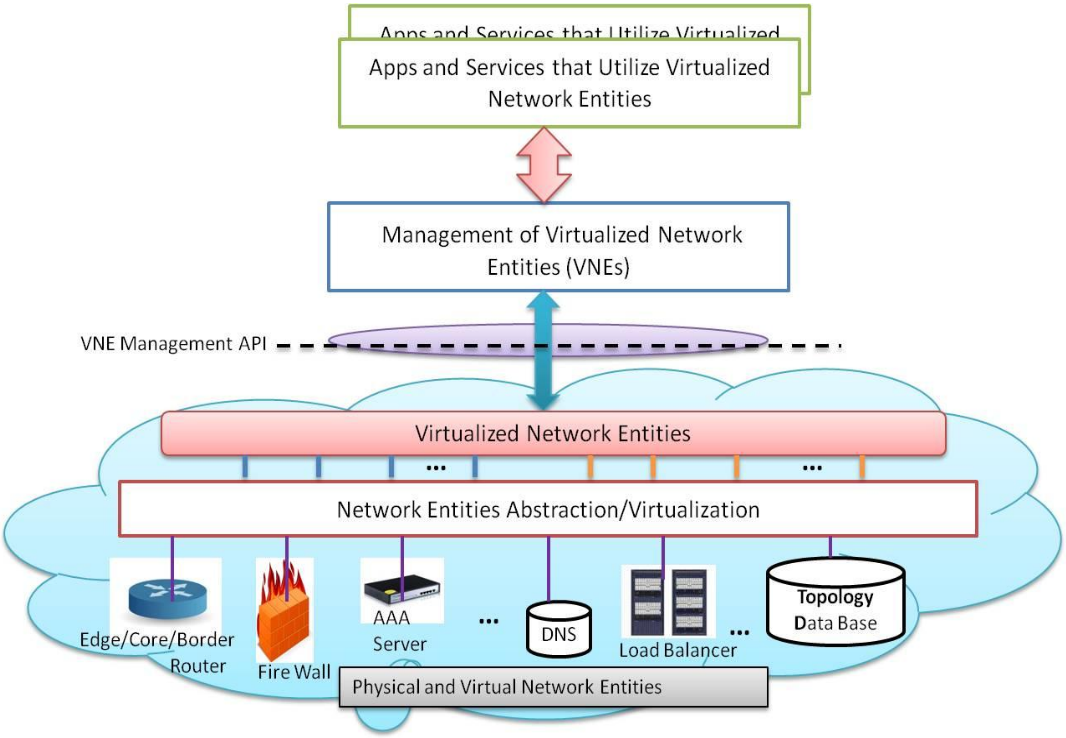

Apps and Services that Utilize Virtualized
Apps and Services that Utilize Virtualized Network Entities
Management of Virtualized Network Entities (VNEs)
VNE Management API
Virtualized Network Entities
...
...
Network Entities Abstraction/Virtualization
Edge/Core/Border Router
Fire Wall
AAA Server
...
DNS
Load Balancer
...
Topology Data Base
Physical and Virtual Network Entities

Figure 1 – Network Entities (Resources and Services) Abstraction, Virtualization and Management

As shown in Figure 1, the followings are the main components of virtualized networking:

- Physical and virtual network elements/entities
- Virtualized network entities (vNEs)
- Application programming interface (API) for vNE management.

4.2.1 Network Entities

The network entities include various network components, such as routers, firewalls, AAA servers, DNS, load balancers, etc. These network components can be interconnected to support network services. Such network entities can be realized both as physical devices or virtual appliances.

A common mechanism for virtualization of these generic network entities is required in order to achieve seamless interoperability. Once virtualization is done, the vNEs can be exposed through open API for management and utilization by various applications and services.

4.2.2 Virtualized Network Entities (vNEs)

The virtualized network entities are the abstraction of the physical network entities and the network entities realized as virtual appliances. The vNEs can be combined flexibly to support virtualized networking services.

These virtualized network entities can be exposed via a management API to the upper management layers. The management API can be used to create, assign, monitor, update, and release the vNEs.

The following sections describe the Use Cases that can be used to derive the management model and required API functions.

5 Network Services Management Use Cases

This section presents the details of a sample of network services management use cases. The details of each use case are presented using the following format.

The Use case Number and Title are mentioned first. This is followed by steps and description per the format shown below. .

i. Short Description

ii. Assumptions (pre-conditions)

iii. Goal(s) / Desired Outcome(s) or post-conditions

iv. Primary, Secondary, and Supporting Actors

v. Triggers and Implementation / required steps for execution (interactions)

vi. Failure Condition(s) and Recovery

vii. Possible Extensions/variations

viii. Non-functional requirements, if applicable

ix. Known issues

5.1 Use Case 1 (UC-1): Pre-defined Template-based Network Configuration

Use case (UC-1) describes pre-defined template-based network configuration.

5.1.1 Short Description of the Use Case

In this use case the end users are not concerned with the details of network topology. The network service required by VMs can be predefined in network templates. For example, the cloud service provider can define standard network topology and network service for a three-tier website.

To build a web site in the cloud, users can select the predefined three-tier website and assign roles, such as front-end web server, application server or database server, to VMs. Once the VM roles are assigned, the high-level network services can be automatically provisioned to these VMs. For example, Firewalls may be setup between web servers and application servers or between application servers and database servers to enforce access control of these servers. Furthermore, load balancer acting as front-end web servers can be automatically configured to distribute external requests to VMs.

From network providers' view, the network template and role assignment information provided by users should be mapped to configurations on physical network devices and VMs (when network services are provided by software). Cloud service provider should have capability to manage network topology/flows/services so that the most frequently utilized network architectures can be deployed inside the virtual network environment.

5.1.2 Assumptions and Pre-Conditions

It is assumed that cloud service providers have developed predefined network topology and service templates, e.g., two-tier website, three-tier website, computing clusters.

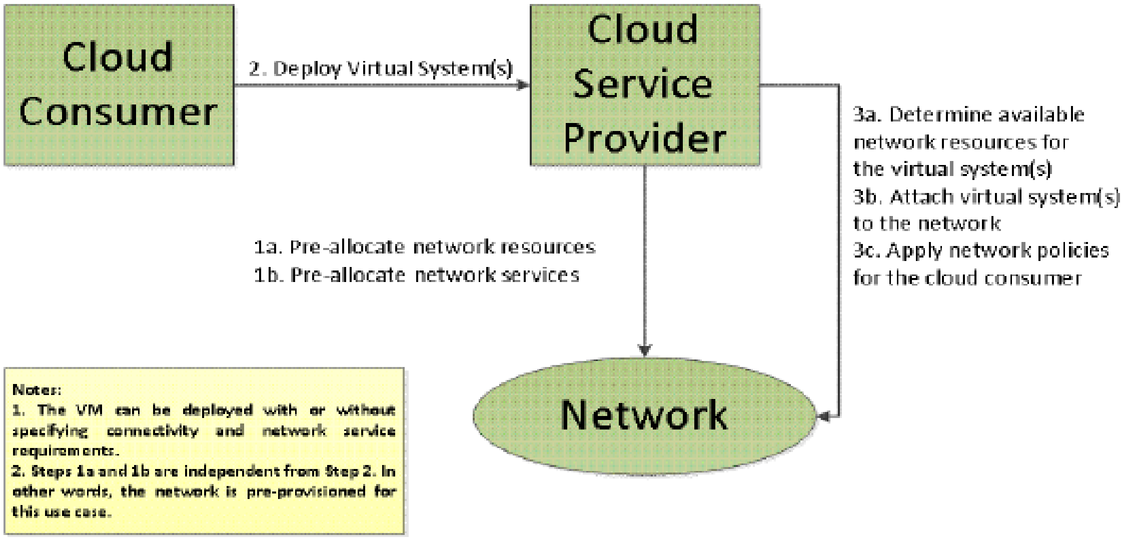

Cloud Consumer
2. Deploy Virtual System(s)
Cloud Service Provider
3a. Determine available network resources for the virtual system(s)
3b. Attach virtual system(s) to the network
3c. Apply network policies for the cloud consumer
1a. Pre-allocate network resources
1b. Pre-allocate network services
Network
Notes:
1. The VM can be deployed with or without specifying connectivity and network service requirements.
2. Steps 1a and 1b are independent from Step 2. In other words, the network is pre-provisioned for this use case.

Figure 2 – Pre-Condition for Network Service Management Use Case 1 (UC-1)

Figure 2 shows one possible way the Cloud Service Providers can prepare and configure their network and services for utilization by the Cloud Consumers for this use case.

5.1.3 Goal(s) and Desired Outcome(s)

The objective is to provide on-demand virtual network to support the cloud consumer application.

5.1.4 Primary, Secondary, and other Supporting Actors

Primary Actor: Cloud Consumer (End User), as defined in the DMTF CIMI spec. and in the definition section (Section 1).

Secondary Actor: Cloud Service Provider

5.1.5 Triggers and Implementation / Executions Steps (Interactions)

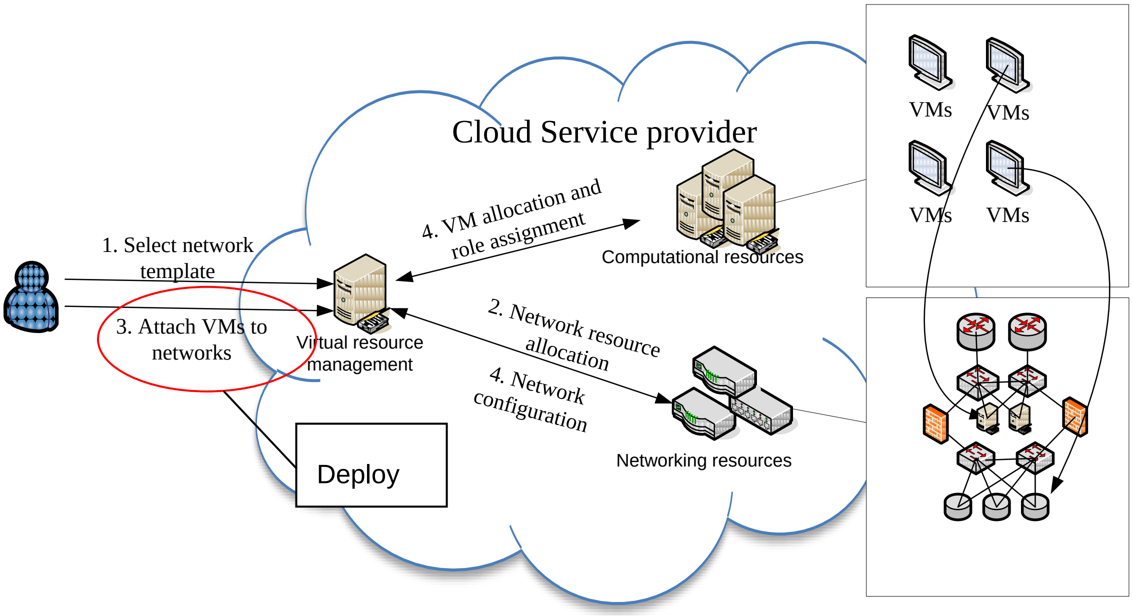

Cloud Service provider
1. Select network template
3. Attach VMs to networks
Virtual resource management
4. VM allocation and role assignment
Computational resources
2. Network resource allocation
4. Network configuration
Networking resources
Deploy
VMs
VMs
VMs
VMs

Figure 3 – High-level Network Service Management Use Case 1 (UC-1)

UC-1 is invoked by the cloud consumer (end user):

1) End user browses the network templates (a topology with connectivity and services) provided by cloud service provider and selects one of the templates. End user sends commands to service provider, requesting a network to be deployed based on the selected template. Specific template configurations may be set by the end user.

2) Cloud service provider deploys the requested network along with the network services based on the predefined network template selected by user. Cloud service provider associates VMs to network ports on the virtual network.

3) End user deploys VMs on the network or associates existing VMs to the network.

4) Cloud service provider associates VMs to Network services configured in the template (or automatically provisioned to the VM based on the role of VM).

The requirements related to UC-1 include the following ones:

- UC-1: Req.-1: Service provider should be able to configure the network based on network service requirements.

- UC-1: Req.-2: Service provider should provide network templates for users which can be easily mapped to popular network topologies.

- UC-1: Req.-3: Service provider may define common network policy services, e.g., Load balancer, FW, on the network templates.

- UC-1: Req.-4: Service provider may scale the capability of network services, e.g., bandwidth/packet processing capability, based on user network requirements.

5.1.6 Failure Condition (s) and Recovery

Failure occurs when the Cloud Service Provider cannot meet the consumer requirements or the request is in violation of one of the business agreement requirements. Failure may also occur when the Service Provider can’t fulfill any one of the implementation steps or triggers discussed in the previous section. In some situations, failure may also occur when the alternatives suggested by the Cloud Service Provider are not acceptable to the Cloud Consumer.

5.1.7 Possible Extensions/variations

Focus on provider-defined pre-configured templates only. The consumer can pick and choose but not modify the templates. For now the consumer-defined templates are out of scope.

5.1.8 Non-functional requirements, if applicable

None, for this version of this document.

5.1.9 Known Issues

None, for this version of this document.

5.2 Use Case 2 (UC-2): Network Configuration based on Existing Physical Network Topology of User’s Data Center

Use case (UC-2) discusses Network configuration based on existing physical network topology of user’s data center.

5.2.1 Short Description of the Use Case

Cloud consumer may have already deployed their own private network and server clusters. When users move their existing IT infrastructures to the cloud, network services in the existing physical networks should also be moved to the virtual network so that VMs migrated from existing physical servers can work properly. In this use case, users should first extract network service configurations, such as ACLs in Firewall and policy settings in Load balancer, from the deployed physical network.

To facilitate the network migration, users may map their network configurations to a standardized format or template, e.g., network service model in CIMI interface or OVF 2 package. After the virtual network is setup by the cloud service provider, user can “plug-in” the VMs seamlessly to the virtual network interfaces mapped to their existing physical network.

5.2.2 Assumptions and Pre-Conditions

Cloud consumer (end user) has already deployed enterprise network.

Cloud consumer (end user) has tools to extract network topology and configurations from existing network.

Cloud consumer Administrator (Admin on the consumer side) has the necessary tools and capability to administer the network and service requests from the Cloud consumer.

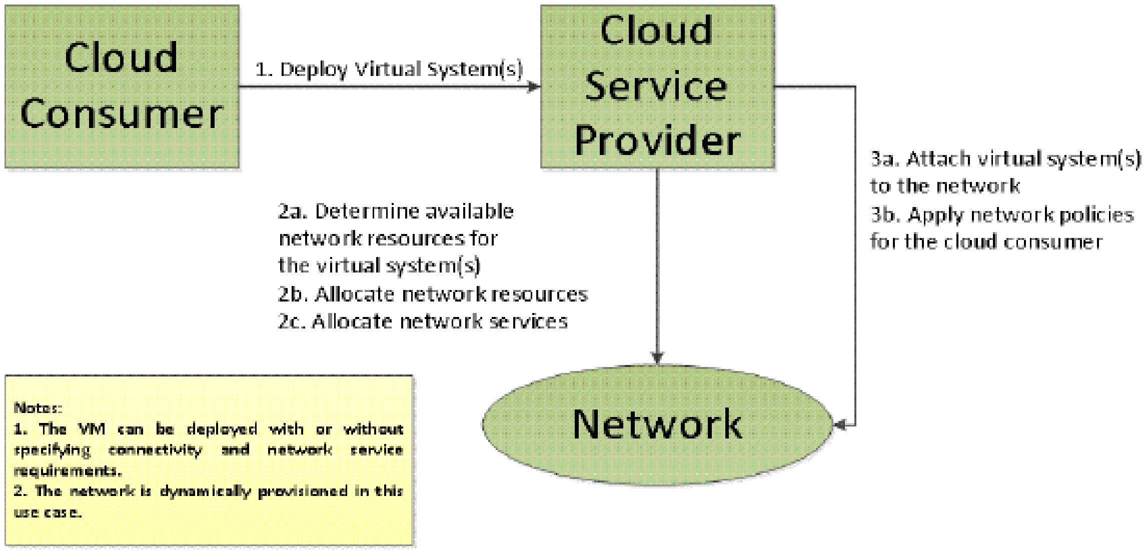

Cloud Consumer
1. Deploy Virtual System(s)
Cloud Service Provider
3a. Attach virtual system(s) to the network
3b. Apply network policies for the cloud consumer
2a. Determine available network resources for the virtual system(s)
2b. Allocate network resources
2c. Allocate network services
Network
Notes:
1. The VM can be deployed with or without specifying connectivity and network service requirements.
2. The network is dynamically provisioned in this use case.

Figure 4 – Pre-Condition for Network Service Management Use Case 2 (UC-2)

Figure 4 shows one possible way the Cloud Service Providers can prepare and configure their network and services for utilization by the Cloud Consumers for this use case.

5.2.3 Goal(s) and Desired Outcome(s)

The objective is to support effortless migration from an existing network to a virtual network by extracting the required network topology and configuration information. The cloud service provider essentially “clones” the existing networking functions and services for seamless migration of resources from one provider domain to another.

5.2.4 Primary, Secondary, and other Supporting Actors

Primary Actor: Cloud Consumer (End User)

Secondary Actor: Cloud Service Provider

Supporting Actor: Cloud Consumer Administrator (Admin)

5.2.5 Triggers and Implementation / Executions Steps (Interactions)

From the cloud service providers’ view, they should get network topology and service configuration information from users. Then they should configure network services (on physical network devices or on VMs) to mimic the network as in the way described by the user. If the service cannot be configured as requested by the users, the cloud service provider should return the reason for the failure and the difference between the configuration of the virtual network and the network requested by the user.

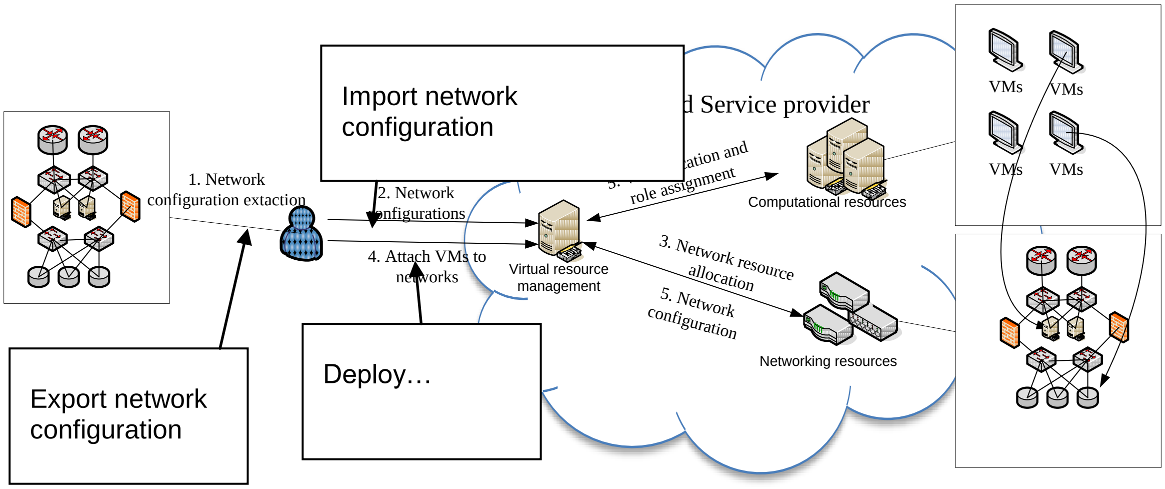

Import network configuration
d Service provider
VMs
VMs
VMs
VMs
1. Network configuration extaction
2. Network onfigurations
ation and role assignment
Computational resources
3. Network resource allocation
4. Attach VMs to networks
Virtual resource management
5. Network configuration
Networking resources
Export network configuration
Deploy…

Figure 5 – High-level Network Service Management Use Case 2 (UC-2)

UC-2 is invoked by the Cloud Consumer Admin:

1) Cloud Consumer Admin exports network topology and configuration from the existing network. The network configuration for specific network services should be mapped to standardized network services.

2) Cloud Consumer Admin imports the network topology and configuration to the cloud service provider.

3) Cloud service provider configures network devices, servers or VMs to setup virtual network and network services which meet the end user's requirements.

4) Cloud Consumer Admin deploys VMs on the network or associates existing VMs to the network.

5) Cloud service provider associates VMs to network ports on the virtual network.

The requirements related to UC-2 include the following ones:

- UC-2: Req.-1: as defined in UC-1: Req.-1.
- UC-2: Req.-2: Service provider should provide interfaces for user to import network topology and configurations.
- UC-2: Req.-3: Service provider should meet user's network requirements by allocating network resources and configure them as requested by the user. If user's requirements cannot be fulfilled, service provider may return the difference between user's requirements and the allocated network resources.
- UC-2: Req.-4: Service provider may provide a set of network services, e.g., routers/FW/LB.
- UC-2: Req.-5: Service provider may enable configuration mechanisms to allow user to migrate configuration data. The configuration may include network services policies, e.g. ACLs in firewall or policies in Load Balancer.

5.2.6 Failure Condition (s) and Recovery

Failure occurs when the Cloud Service Provider cannot meet the consumer requirements or the request is in violation of one of the business agreement requirements. Failure may also occur when the Service Provider can't fulfill any one of the implementation steps or triggers discussed in the previous section. In some situations, failure may also occur when the alternatives suggested by the Cloud Service Provider are not acceptable to the Cloud Consumer.

5.2.7 Possible Extensions/variations

Cloud service provider may return the difference between available virtual network capability and user request when any significant parts of user's requirements cannot be fulfilled.

5.2.8 Non-functional requirements, if applicable

Users may request for specific capacity for a given network service, e.g., a Firewall may need to have black list size larger than 10,000 entries and should be able to process 1M packets per second. These types of features are commonly supported.

5.2.9 Known Issues

None, for this version of this document.

5.3 Use Case 3 (UC-3): Network Configuration Modification

Use case 3 (UC-3) illustrates network configuration modification during run time.

5.3.1 Short Description of the Use Case

A cloud consumer administrator may need to modify the network configuration while their virtual systems are running.

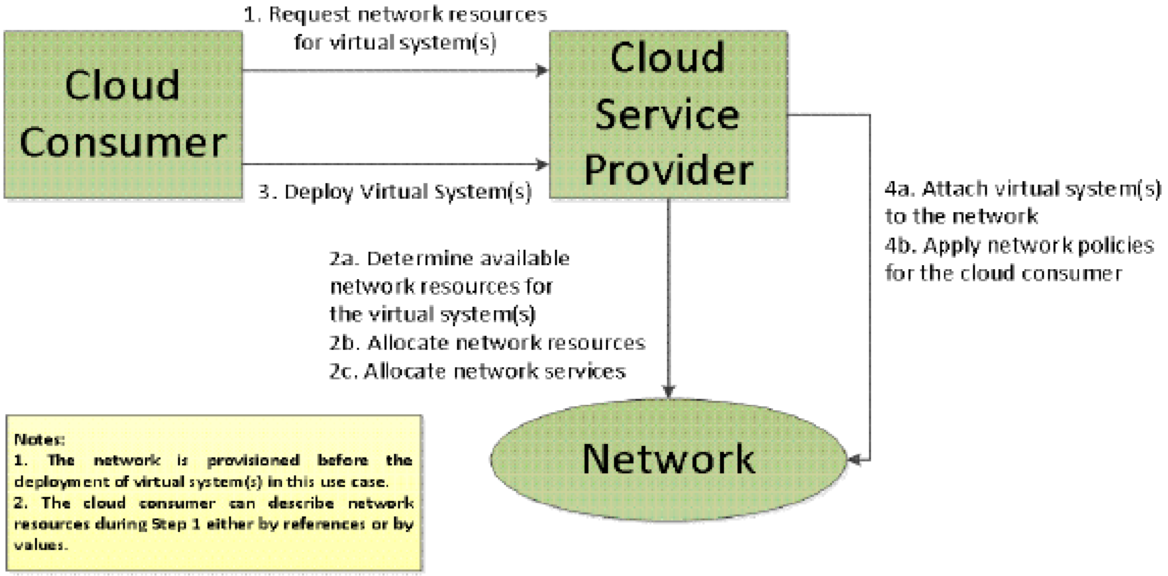
For example, changes may be needed to the ACLs in firewall or scaling the network based on workload demand.

The cloud consumer administrator can use the CIMI interface to request changes in the network configuration.

5.3.2 Assumptions and Pre-Conditions

The cloud service provider has deployed the virtual network as requested by the cloud consumer administrator.

The cloud consumer administrator has the necessary tools to effect changes.


Cloud Consumer
1. Request network resources for virtual system(s)
Cloud Service Provider
3. Deploy Virtual System(s)
4a. Attach virtual system(s) to the network
4b. Apply network policies for the cloud consumer
2a. Determine available network resources for the virtual system(s)
2b. Allocate network resources
2c. Allocate network services
Network

Notes:
1. The network is provisioned before the deployment of virtual system(s) in this use case.
2. The cloud consumer can describe network resources during Step 1 either by references or by values.

Figure 6 – Pre-Condition for High-level Network Service Management Use Case 3 (UC-3)

Figure 6 shows one possible way the Cloud Service Providers can prepare and configure their network and services for utilization by the Cloud Consumers for this use case.

5.3.3 Goal(s) and Desired Outcome(s)

The objective is to achieve an on-demand update of the network configuration. This facilitates dynamic addition/removal/modification of network capacity, service quality, and capabilities of the services.

5.3.4 Primary, Secondary, and other Supporting Actors

Primary Actor: Cloud Consumer

Secondary Actor: Cloud Service Provider

Supporting Actor: Cloud Consumer Administrator

5.3.5 Triggers and Implementation / Executions Steps (Interactions)

From the cloud service providers' view, they must provide automatic network service reconfiguration, in addition to user requested configuration changes. Such automatic network service reconfiguration includes: automatically relocate network services when there is a network failure, automatically scale up network service capacities when more VMs or computational resources are allocated to the user.

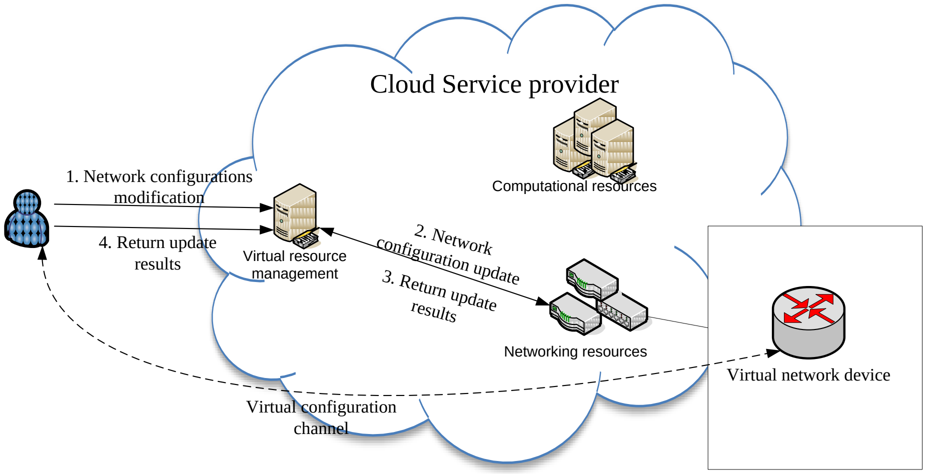


Figure 7 – High-level Network Service Management Use Case 3 (UC-3)

UC-3 is invoked by the cloud customer administrator:

1) The cloud consumer administrator sends a request to the cloud service provider to modify a network service configuration.

2) The cloud service provider modifies the network service configuration.

3) The cloud service provider returns the status of the network service configuration change to the cloud consumer administrator.

4) The cloud consumer administrator verifies that the requested modification has been made.

The requirements related to UC-3 include the following ones:

- UC-3: Req.-1: The cloud service provider is able to accept requests for network service configuration changes from the cloud consumer administrator.

5.3.6 Failure Condition (s) and Recovery

A failure occurs if the cloud service provider cannot support the requested network service configuration change.

5.3.7 Possible Extensions/variations

None, for this version of this document.

5.3.8 Non-functional requirements, if applicable

None, for this version of this document.

5.3.9 Known Issues

None, for this version of this document.

6 Relationships with DMTF Specifications

In this section, a short overview of the DMTF specifications and models related to networking is presented.

6.1 OVF

Open Virtualization Format Specification (DSP0243)

OVF describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines. The OVF package contains Network Section which describes logical networks used in the package. Connections to Networks are specified through configurations on Ethernet Adaptors.

6.2 CIMI

Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP specification (DSP0263)

CIMI focuses on the model and protocol for management interactions between a cloud Infrastructure as a Service (IaaS) Provider and the Consumers of an IaaS service. Among other resources, such as Machines and Volumes, CIMI also provides management for Networking resources, which include Network, Network Template, Network Configuration, Network Port, Network Port Template, Network Port Configuration, Address, Address Template, Forwarding Group, Forwarding Group Template and their respective collections.

CIMI needs to be able to support implementing the subset of the requirements of the use cases described in this white paper as applicable to the Provider/Consumer interface.

6.3 Network Related Profiles

DMTF defined network related management profiles include: Virtual System Profile (DSP1057), Ethernet Port Profile (DSP1014), Resource Allocation Profile (DSP1041), Allocation Capabilities Profile (DSP1043), Ethernet Port Resource Virtualization Profile (DSP1050), and Virtual Ethernet Switch Profile (DSP1097).

Network management is an important component for the management task. The current DMTF standards mostly focus on network aspects of L2 and below networks, which mainly involves with network ports, adaptors, L2 switches, etc. For a more complete view of networking management, L3 and above network services should be considered.

7 Impact to the existing DMTF Specifications

Table 1 shows the potential impact on the CIMI interface, OVF, and NPP based on the requirements developed above.

Table 1 – Potential Impact to the DMTF Specifications

Requirement	DMTF Spec Usage	Comments
UC-1: Req.-1	OVF: Supported	Cloud Service Provider pre-configures the relationship among NPP, VM/VNE, and Topology
	CIMI: Show network resource capability (need more granularity and flexibility)	
	NPP Schema: VMs and VNEs are included into the network topology. End user selects topology and related Network Port Profiles (NPPs) from the Port Profile Database (PPDB)	
UC-1: Req.-2	OVF: Network resources selection and assigning VM to the network. Basic functions are available in OVF 1.x and OVF 2.0; advanced functions (quality of service, load balancer, fire wall) will be available in post OVF 2.0)	NPP is layer-2 related configuration data which can be used to configure the port of VM. This needs to be extended to support layer-3 parameters and entities. Otherwise, may need to initiate a new work item
	CIMI: Template selection, and mapping requirements to the template	
	NPP Schema: Network templates provided by Cloud Service provider should include VMs/VNEs associated NPPs which can be taken from the Port Profile Database (PPDB)	
UC-1: Req.-3	OVF: Network (L2 and above) service extension (available in post OVF 2.0)	If common network policy services are not related to new VM/VNE deployment, or there is no need to change NPP to support these services
	CIMI: Network (L2 and above) service extension (may leverage OVF specs.)	
	NPP Schema: No direct relationship	
UC-1: Req.-4	OVF: Scaling policy definition (out of scope; need more discussion)	If the capability scaling of network services is not related to new VM/VNE deployment or there is no need to change NPP to support the capability scaling
	CIMI: Scaling policy definition (out of scope; need more discussion)	
	NPP Schema: No direct relationship	
UC-2: Req.-1	OVF: Same as in UC-1: Req.-1	Cloud Service Provider pre-configures the NPPs for the VM/VNE included into the standardized network services
	CIMI: Same as in UC-1:Req.-1	
	NPP Schema: Cloud Service Provider need to take port related configuration data from end user provided network topology and configuration, and construct these into VM/VNE related NPP, or should get the pre-configured NPP based on the standardized network services which are mapped from the specific physical network services	
UC-2: Req.-2	OVF: Add new configuration and detailed network parameters	Cloud Service Provider pre-configures the NPPs for the VM/VNE included into the standardized network services
	CIMI: Add new configuration and detail network parameters	
	NPP Schema: NPP can be constructed based on the configuration data provided by the End user from the interfaces, or can bind to some pre-configured NPP based on the standardized network services which are mapped from the specific physical network services	

UC-2: Req.-3	OVF: Supported	If the port profiles can't be supported per End User's network requirements, Cloud service provider should return the difference at network service level
	CIMI: Return differences when user requirements cannot be met (outside the scope)	
	NPP Schema: Cloud Service Provider needs to check whether the platform can support the required port configuration data based on End User's network requirements	
UC-2: Req.-4	OVF: Define standard network services (limited support)	If a standard network service is supported by VM/VNE, the affected port configuration data related to the network service should be reflected into NPP
	CIMI: Define standard network services (not available as an API; only through OVF import)	
	NPP Schema: Cloud Service Provider should provide mapping of standard network services to some port configuration data of NPP	
UC-2: Req.-5	OVF: Network device configuration parameters (limited support)	None
	CIMI: Network device configuration parameters (not available as an API; only through OVF import)	
	NPP Schema: Migration of configuration data has no direct influence on the content of NPP, but impact the location only	
UC-3: Req.-1	OVF: Not Supported, Runtime features to be supported in future version.	If some network capability is auto-scaled by Cloud Service provider, the affected port configuration data in NPP should be modified
	CIMI: Supported. May provide network service configuration interface through CIMI	
	NPP Schema: Cloud Service Provider should provide mapping of network capability to some port configuration data of NPP. NPP should be modified to support the network services configured by the End User	
	CIMI: May return network service configuration interface through CIMI	
	NPP Schema: NPP should be modified to support the network services configured by the End User	

ANNEX A
(Normative)

IETF/IRTF Standards and Specifications

The following three active IETF (http://datatracker.ietf.org/wg/) and IRTF (http://www.irtf.org/groups) working groups may be most relevant to the DMTF NSM WG:

- Network Virtualization Overlays (NVO3) in the Routing Area (RA) of IETF
- System for Cross-domain Identity Management (SCIM) in the Applications Area (AA) of IETF
- Software Defined Networking Research Group (SDN-RG) in IRTF

A brief description of each of the above groups is presented below.

NVO3: It is noted that support for multi-tenancy has become a core requirement of data centers (DCs), especially in the context of data centers supporting virtualized hosts and virtual machines (VMs). The NVO3 WG will investigate the interconnection of the DC virtual private network (VPNs) and their tenants with non-NVO3 Internet protocol-based network(s) to determine if any specific work is needed. Further details about the charter of NVO3 can be found at the following Website: http://datatracker.ietf.org/wg/nvo3/charter/.

SCIM: SCIM working group will standardize methods for creating, reading, searching, modifying, and deleting user identities and identity-related objects across administrative domains, with the goal of simplifying common tasks related to user identity management in services and applications. Further details about the charter of NVO3 can be found at the following Website: http://datatracker.ietf.org/wg/scim/charter/.

SDN-RG: SDN-RG provides a forum for researchers to investigate key and interesting problems in the Software Defined Networking (SDN) field. It investigates SDN from various perspectives with the goal of identifying the approaches that can be defined, deployed and used in the near term as well identifying future research challenges. Key areas of interest include solution scalability, abstractions, and programming languages and paradigms particularly useful in the context of SDN. Further details about the charter of SDN-RG can be found at the following Website: http://trac.tools.ietf.org/group/irtf/trac/wiki/sdnrg.

ANNEX B
(Informative)

(Inter-Provider Use Case)

B.1 Use Case B1 (UC-B1): Location Aware Hosting of Virtual Desktop

This is an Inter-Provider use case. This use case (UC-B1), describes location aware hosting of Virtual Desktop (VD).

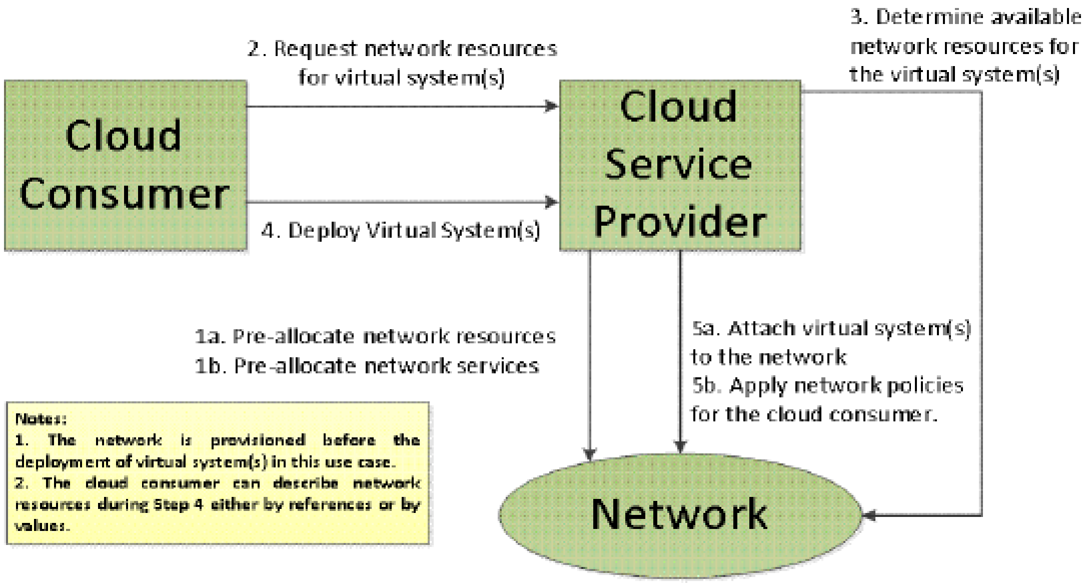
B.1.1 Short Description of the Use Case

Implementation of this use case facilitates accessing of the features and services by a roaming virtual desktop (VD) without directly using a virtual machine (VM) in a host of the original home/Enterprise Data center.

B.1.2 Assumptions and Pre-Conditions

A virtual desktop (VD) client is installed in a device (Tablet, Mobile phone, Laptop, phablet, etc.) that can travel with the user, and the user can get all of the services and features seamlessly irrespective of the location through generic network (Internet) access.

In general, the VD is hosted in a virtual machine (VM) in the Enterprise (private) Data Center (DC). When the user is roaming, another VM in a visited DC may host the VD


Cloud Consumer
2. Request network resources for virtual system(s)
Cloud Service Provider
3. Determine available network resources for the virtual system(s)
4. Deploy Virtual System(s)
1a. Pre-allocate network resources
1b. Pre-allocate network services
5a. Attach virtual system(s) to the network
5b. Apply network policies for the cloud consumer.
Network

Notes:
1. The network is provisioned before the deployment of virtual system(s) in this use case.
2. The cloud consumer can describe network resources during Step 4 either by references or by values.

Figure 8 – Pre-Condition for High-level Network Service Management Use Case B1 (UC-B1)

Figure 8 shows one possible way the Cloud Service Providers can prepare and configure their network and services for utilization by the Cloud Consumers for this use case.

B.1.3 Goal(s) and Desired Outcome(s)

The objective is to achieve on-demand hosting and mobility support for virtual desktop. The virtual desktop features and host (in VM) location are adapted based on network and service access location. This helps achieve the desired performance to the visited location. It is required to share cross-domain topology and resource utilization information in order to achieve the desired optimization.

B.1.4 Primary, Secondary, and other Supporting Actors

Primary actors: Cloud consumers who have Virtual desktop (VD) client, VD host, Networking as a Service (NaaS) proxy, etc.

Secondary actors: Cloud service provider with the capability to support Networking as a Service (NaaS) server, virtual machine, Host, Data center, etc.

Supporting actors: Service monitoring/management/logging/auditing tools, and associated infrastructure.

B.1.5 Triggers and Implementation / Executions Steps (Interactions)

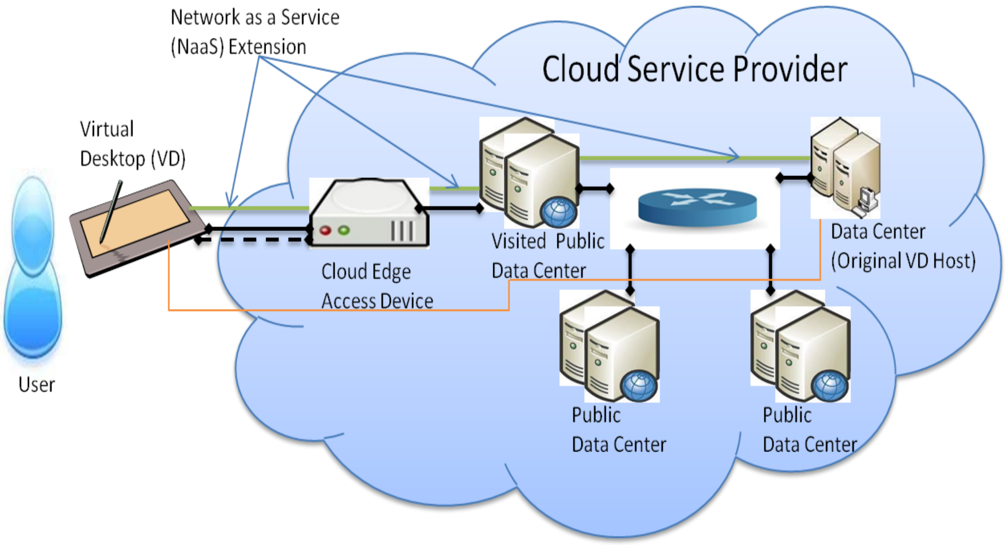


Figure 9 – High-level Network Service Management Use Case B1 (UC-B1)

An implementation of UC-B1 can be invoked by any cloud customer (end user) who has a VD installed in a network (Internet) access capable device, e.g., tablet, laptop, mobile phone, etc. The following are possible high-level steps:

1) Turn on the device and activate the virtual desktop (VD).

2) Enable network (Internet) access.

3) Start the Web Browser, and Type-in the URL for accessing the VM in the Enterprise Data center that is hosting the VD.

4) Provide the valid LogIn credentials for access verification/challenge, and then allow successful Login or report mis-handling of the system, unauthorized access attempts, etc.

5) Enterprise Data center recognizes the current roaming location of the VD and locates a nearby guest Data Center and a VM in that DC that can host the VD.

6) The guest DC then establishes back-end Network as a Service (NaaS) extension to the VM in the original Enterprise DC

7) The VD which is now hosted in a VM in the guest DC, and it can have all of the service and features as in the original DC without having direct access to the VM in the original Enterprise DC

8) Service usages are monitored and recorded for logging, auditing and QoS/QoE maintenance purposes

9) When the user logs off, the VM, NaaS, and associated resources form eth guest DC are released, and all of the recorded service logging and auditing related data are transferred back to the original Enterprise DC.

The requirements related to UC-B1 include the following ones:

- UC-B1: Req.-1: The device that contains a valid/registered VD should be able to establish a VPN or layer-2 tunnel to the Enterprise Data Center (DC) where the original VM that hosts the VD resides.

- UC- B1: Req.-2: Based on the physical location of the VD, the Original DC (in collaboration with the VM that is Hosting the VD) should be able to determine -- based on many criteria, and one of these may be the geographical proximity of the VD-device – a guest/visited DC, and must locate a VM (within the DC) which can host the VD temporarily (for the duration of the session). Note that a federation of VMs may be used to locate a feasible VM to Host the VD as well (cross-domain resources discovery and topology sharing may be required for this purpose).

- UC- B1: Req.-3: Original VM should be able to negotiate for the desired features and services of the VD with the VM in the guest/visited DC. If the negotiation passes, a VM is located in the desired DC to Host the VD. If not, the Enterprise DC should be able to locate an alternative DC within a given set of constraints, and a VM is located in it to host the VD (cross-domain resources discovery and topology sharing may be required for this purpose).

- UC- B1: Req.-4: VM in the guest/visited DC should be able to establish VPN or Layer-2 tunnel (back-end networking as a service or NaaS extensions) to the VM in the original Enterprise DC VM (VD-host).

- UC- B1: Req.-5: Back-end NaaS extensions should be able to allocate, monitor and enforce the features and services including QoS/QoE, privacy and security requirements, and must facilitate logging and auditing data collection throughout the session. The features may utilize virtualized computing, communications, storage, transcoding, etc. resources.

- UC- B1: Req.-6: The VD should now be able to access the VM (Host) in the guest/visited DC and must have access to all of the features and functions as if the VD (VM) is in the original Enterprise DC that hosts the VD.

- UC- B1: Req.-7: It is required to support the abstraction of cross-DC (among the VMs that are Hosting the VD) communications.

- UC- B1: Req.-8: It is required to support the abstraction of cross-DC (among the VMs that are Hosting the VD) co-ordination of VD features and services.

- UC- B1: Req.-9: It is required to support the availability of Topology and Cost (delay, jitter, loss, price, etc. matrix) data across the desired DC domains.

B.1.6 Failure Condition (s) and Recovery

In general, failure occurs when the Cloud service provider cannot support the desired network-aware hosting of virtual desktop. In addition, failure may occur when the Cloud Service Provider cannot satisfy any one of the implementation steps or triggers discussed in the previous section. This may include regulatory restrictions, and lack of availability of VM features/functions/capability in the visited hosts.

B.1.7 Possible Extensions/variations

The roaming user may provide some preference regarding the location of the guest DC. Similarly, the Enterprise DC may have a set of pre-selected list of globally distributed DCs from which the guest DC can be selected.

It is possible that service-specific QoS/QoE and security profile will be invoked either by the VD or by the VM or by both.

If desired, logging of auditable service usage may be flexible as well.

B.1.8 Non-functional requirements, if applicable

The non-functional requirements for this use case may include the following: (a) personalization of VD and VM profiles, (b) service granularity and quality, and (c) service usage capacity including bandwidth and volume/size of downloaded/uploaded data.

B.1.9 Known Issues

None, for this version of this document.

B.2 Impact to the existing DMTF Specifications

Table 2 shows the potential impact on the CIMI interface, OVF, and NPP based on the requirements developed above for this Inter-Provider use case.

Table 2 – Impact to DMTF Specifications for an Inter-Provider Use Case

UC-B1: Req.-1	OVF: Supported	NPP exists in the Enterprise Data Center (DC) where the original VM that hosts the VD resides
	CIMI: Per-user authentication, VM assignment and access	
	NPP Schema: No special requirements	
UC-B1: Req.-2	OVF: On demand VPN setup	NPP may be migrated to the guest/visited DC environment
	CIMI: On demand VPN setup	
	NPP Schema: NPP of the VM that is Hosting the VD should be supported and provided in the guest/visited DC which provides a feasible VM to Host the VD	
UC-B1: Req.-3	OVF: None	
	CIMI: Inter-DC negotiation	
	NPP Schema: Cloud Service Provider should support mapping of features and services of the VD with the VM/VNE to some port configuration data of NPP	
UC-B1: Req.-4	OVF: On demand VPN setup QoS guarantee	NPP can be accessed to and configured in VM/VNE in both guest/visited DC and the original Enterprise DC
	CIMI: On demand VPN setup QoS guarantee	

	NPP Schema: No special requirements	
UC-B1: Req.-5	OVF: Supported	None
	CIMI: Extension on metering	
	NPP Schema: Cloud Service Provider should support mapping of the features and services of the NaaS extensions to some port configuration data of NPP	
UC-B1: Req.-6	OVF: Supported	NPP can be accessed to and configured in VM/VNE in both guest/visited DC and the original Enterprise DC
	CIMI: Supported	
	NPP Schema: No special requirements	
UC-B1: Req.-7	OVF: Supported	NPP can be accessed to and configured in VM/VNE in both guest/visited DC and the original Enterprise DC
	CIMI: On demand VPN setup	
	NPP Schema: No special requirements	
UC-B1: Req.-8	OVF: Supported	The port profiles can be coordinated between the guest/visited DC and the original Enterprise DC
	CIMI: Inter-DC coordination	
	NPP Schema: Cloud Service Provider should provide mapping of the features and services of the VD with the VM to some port configuration data of NPP	
UC-B1: Req.-9	OVF: Supported	The supported port profiles across the desired DC domains need to be checked
	CIMI: Inter-DC data sharing	
	NPP Schema: Cloud Service Provider should support checking and mapping of the Topology and Cost data to some port configuration data of NPP	

ANNEX C
(Change Log)

Version	Date	Description
wgv0.1.0-	2012-08-11	Early Template and Outline
wgv0.1.1-	2012-08-17	Initial Draft
wgv0.1.2-	2012-08-26	Updated with Use Case Details
wgv0.2.0-	2012-09-07	Updated with Edits and Use Case Details
wgv0.2.1-	2012-09-07	Updated with Edits/Clarification
wgv0.2.2-	2012-09-10	Updated with Edits/Clarification
wgv0.2.3-	2012-09-19	Updated to address the comments from face-to-face mtg. and discussion
wgv0.3.0-	2012-09-28	Updated pre-condition and definition section
wgv0.4.0-	2012-10-03	Edits and updates
wgv0.4.1-	2012-10-12	Edits and updates
wgv0.5.0-	2012-10-16	Converted to DMTF template
wgv0.5.1	2012-10-19	Worked on terms and definitions
wgv0.5.2	2012-10-24	Added DSP number and some formatting
wgv0.5.3-9	2012-10-25	Edits and updates
wgv 0.6.0	2012-01-16	WIP release candidate
1.0.0a wgv 0.6.1	2012-01-17	WIP release candidate with footer, front, page, references fixed.
1.0.0a	2013-03-20	WIP release