# Network Port Profiles Based Provisioning and Deployment Models for Virtual Networking

Hemal V. Shah
Infrastructure and Networking Group
Broadcom Corporation
Irvine, California, USA
hemal@broadcom.com

John Parchem
Microsoft Corporation
Redmond, Washington, USA
John.Parchem@microsoft.com

Shishir Pardikar
Citrix Corporation
Seattle, Washington, USA
Shishir.Pardikar@citrix.com

Lawrence Lamers
VMware
San Jose, California, USA
ljlamers@vmware.com

***Abstract*—A network port profile is an XML document that describes a set of networking attributes that can be applied to Ethernet ports and virtual Ethernet switches. This paper describes network port profile XML schema and Open Virtualization Format (OVF) standards based provisioning and deployment models for virtual networking components that address challenges associated with multiple and separate virtual networking management domains.**

***Keywords-network port profile; OVF; virtual networking; virtual networking management***

## I. INTRODUCTION

Virtual networking enables connectivity between the virtual computer systems that are networked together. Virtual computer systems connect to each other and to the network using virtual Ethernet ports and virtual Ethernet switches. In today's data center, multiple and separate virtual networking management domains exist. These virtual networking management domains are typically managed by different administrators. This leads to several challenges in the current virtualized environments including lack of common configuration information that may be referenced by the virtualization ecosystem management entities and possibly inconsistent configuration of managed objects that overlap management domains.

A network port profile is an XML document that describes a set of networking attributes that can be applied to Ethernet ports and virtual Ethernet switches. This paper describes network port profile standards based provisioning and deployment models for virtual networking components that address challenges associated with multiple and separate virtual networking management domains.

First, an overview of Network Port Profile XML Schema is provided. This schema can be used to consistently represent networking attributes of a virtual computer system or a set of virtual computer systems. The application of network port profile to a virtual machine results in a specific configuration of the network infrastructure to which the virtual machine gets connected. Second, extensions to Open Virtualization Format (OVF) for the incorporation of network port profiles are described. This allows the packaging and distribution of networking attributes for a set of virtual computer systems using a common packaging format. Third, the use cases of network port profiles for pre-provisioned and dynamically provisioned physical network infrastructures are described to demonstrate benefits of network port profiles.

## II. BACKGROUND

### A. Terminology

This subsection describes the terminology used in this paper.

*1) Embedded Switch (eSwitch)*

An eSwitch is a virtual Ethernet switch that is embedded in hardware Ethernet Adapter that implements either the Virtual Ethernet Bridge (VEB) or Virtual Ethernet Port Aggregator (VEPA) function as defined in [4].

*2) Local Area Network (LAN)*

A network that connects a group of computer systems in close proximity to each other such as in a building, an office, or a data center.

*3) Network Interface Controller (NIC)*

A NIC is a component that connects a computer system or virtual computer system to a network. It is also referred to as a network adapter or adapter or Ethernet adapter in this paper.

*4) Network Port Profile*

A network port profile is a DSP8049 [3] compliant XML document that describes a set of networking attributes that can be applied to Ethernet ports and virtual Ethernet switches.

*5) Network Port Profile Database (NPPDB)*

The Network Port Profile Database refers to a set of network port profiles stored in a data base.

*6) Physical NIC (pNIC)*

978-3-901882-48-7 

Typically refers to a physical NIC that resides in a physical computer system either as a stand-in card or as a LAN-On-Motherboard (LOM). pNIC may also apply to other physical realizations inside a physical computer system.

*7) Storage Area Network (SAN)*

A SAN is a special-purpose network that interconnects different kinds of storage devices with associated computer systems.

*8) Virtual Ethernet Switch*

A virtual Ethernet switch is an Ethernet switch that provides internal and external network connectivity to the virtual computer systems attached to it. A virtual Ethernet switch implements either the VEB or VEPA function.

*9) Virtual Computer System or Virtual Machine (VM)*

A virtual system as applied to a computer system.

*10) Virtual Network Interface Controller (vNIC)*

An entity that performs the Media Access Control (MAC), Link Level Control (LLC), management and control functions needed to attach a VM to a network.

*11) Virtual Switch (vSwitch)*

Software-emulated virtual Ethernet switch typically implemented within the virtualization infrastructure (e.g., a Hypervisor).

## *B. Management Challenges with Virtual Networking*

In today's data center, multiple and separate management domains for server/workstation (called host, virtualization host, or virtualization platform from here on) exist on LAN and SAN. Additionally, there also exists a separate virtualization specific management domain for virtualized platforms. These management domains have traditionally been managed by different administrators. Figure 1 shows a block diagram of the main components involved in virtual networking.

These separate management domains present several problems in the current virtualized environment including:

*1) Lack of a unified programmatic management interface that spans multiple management domains.*

*2) Possibility of inconsistent configuration of managed objects that overlap management domains – especially managed objects that span virtualization hosts and network infrastructure.*

*3) Lack of common configuration information that may be referenced by the virtualization ecosystem management entities.*

*4) Disparity between the capabilities of embedded bridges in the virtualization hosts and the capabilities of bridges in the attached network.*

The above problems make maintaining a consistent view of a network almost impossible. Furthermore, different tools and mechanisms are required to provision, deploy, and manage different parts of the network. The automation and dynamic provisioning of networks required to support VM migration between physical computer systems become difficult if the above problems are not addressed.

In the past, there have been several proprietary solutions from network switch vendors and/or virtualization software providers to ensure consistent configuration of a network in the virtualized environments. These solutions require the use of proprietary tools from specific vendors as well as the deployment of homogeneous virtual networking components for ensuring consistent configuration. In order to have interoperable solutions to manage virtual networking environments with heterogeneous virtual networking components, there is a need to define standards to address provisioning, deployment, and management of virtual networking components. The next subsections describe the standards defined by the DMTF to address network provisioning, deployment, and management in virtualized environments.

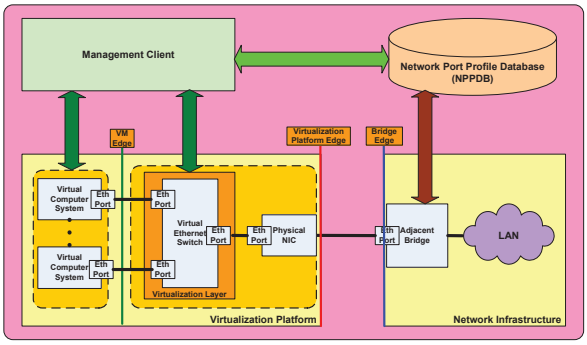


Figure 1. Virtual Networking Management

## *C. Network Port profile*

A Network Port Profile refers to a set of networking attributes that can be applied to one or more virtual machines. The application of a network port profile to a virtual machine results in a specific configuration of the underlying network infrastructure to which the virtual machine gets connected.

There is a need to ensure consistent configuration of these objects for inter-VM traffic that may be switched by a bridge that can be a vSwitch or an eSwitch or an external bridge. Network configuration of the virtual links between the embedded bridge within the virtualization platform and the external attached bridge is stored in a configuration data base called the Network Port Profile Database (NPPDB). The NPPDB provides information that can be used to establish the virtual link between the embedded bridge in the virtualization platform and the attached bridge with a consistent and common configuration data. A management client for example may use this information to rebuild the virtual link when VMs migrate. Likewise the attached bridge manager has access to consistent and common configuration data for its port.

## *D. Network Port Profile XML Schema*

The Network Port-Profile XML schema in [3] defines the structure of Network Port Profile XML documents. The network port profile XML schema provides a common way to represent the elements of network port profiles. Network port profile XML Schema uses the XML elements derived from the properties of Common Information Model (CIM) based class

EthernetPortAllocationSettingData. The use of properties of CIM_EthernetPortAllocationSettingData to represent the standard elements of network port profile enables a consistent representation of network attributes during the packaging, deployment, and runtime management of virtual networking components. The Network Port Profile XML schema is also extensible as it allows the incorporation of other elements that are not derived from the properties of EthernePortAllocationSettingData. The Network Port Profile XML Schema can be used to represent the networking attributes including:

1) *Network Port Profile Identifier*
2) *MAC addresses*
3) *VLANs*
4) *MAC Address/VLAN pairs*
5) *Traffic priority*
6) *Flow control*
7) *Bandwidth settings*
8) *Access Control Lists (ACLs)*

The above list is for illustrative purposes; there may be additional networking attributes that could be represented by network port profiles.

### E. OVF

Open Virtualization Format or OVF is a standard packaging format that provides ease of portability, security, and transportation in order to develop virtual appliances or a pre-configured software stack comprising one or more virtual machines once, and deploy them on a wide variety of platforms. Thus an OVF package may contain a single virtual machine with the corresponding metadata in order to serve as a template within an organization to deploy virtual machines for different user groups, or it may contain multiple VMs representing a more complex application such as a multitier application that is pretested and configured.

An OVF package contains a descriptor and additional content in one or more virtual disks or images in other formats such as ISOs. The content can accompany the OVF descriptor file or can be external to it and referred to via HTTP. The OVF descriptor is an XML document that describes the metadata about the software installed on the virtual disks. The OVF descriptor contains commonly needed metadata organized into sections such as virtual hardware, disks, networks, resource requirements, and customization parameters. The descriptor is designed to be extensible so that further vendor-specific information can be added by extending existing sections or by adding additional sections. The OVF specification allows any virtual disk format to be used, as long as the disk format specification is public and without restrictions.

In order to provide runtime customizability, the OVF specification also provides an OVF environment document specification. The environment document allows a standard and extensible way for a virtualization platform to communicate deployment configuration to the guest software for runtime customization, if necessary. The OVF environment is an XML document containing deployment time customization information for the guest software such as MAC addresses, system UUIDs, IP addresses, etc. The OVF environment document is typically derived from the metadata in the OVF descriptor. The OVF environment document can be provided via a transport mechanism such as a dynamically generated ISO made available to the VM(s) in the appliance during the boot time.

## III. NETWORK PORT PROFILE REPRESENTATION IN OVF

The lifecycle of a Virtual Appliance packed in an OVF includes a) development, b) packing and distribution, c) deployment, d) runtime management, and e) termination. A service, consisting of one or more VMs and the relevant configuration and deployment metadata, is packaged into the OVF format at the end of the development phase. The deployment phase is the installation of an OVF package. The network port profile representation in the OVF provides a standard-based method for provisioning and deployment of virtual networking components of the VMs, virtual network switches, and underlying physical network infrastructure to which the virtual networking components connect to.

As shown in Figure 2, network port profiles can be incorporated in an OVF package in at least three different ways as described below:

*1)* The OVF package can include one or more network port profiles inside the package as separate XML documents, and the OVF file inside the package contains the references to the network port profiles that apply to one or more virtual computer systems or VMs represented in the OVF file.

*2)* The OVF package can contain the network port profiles or the elements of network port profiles embedded inside the OVF file of the package. The embedded network port profile information applies to one or more virtual computer systems or VMs represented in the OVF file.

*3)* The OVF package contains the references to one or more network port profiles that are not contained inside the package. For example, the package uses URIs to reference network port profiles. The referenced network port profiles apply to one or more virtual computer systems or VMs represented in the OVF file.

Network port profile XML schema and OVF together provide a standards-based and interoperable way of provisioning and deploying networks in virtualized environments. The following sections describe how network port profiles can be deployed in pre-provisioned and dynamically provisioned network environments including Software Defined Network (SDN) environments.

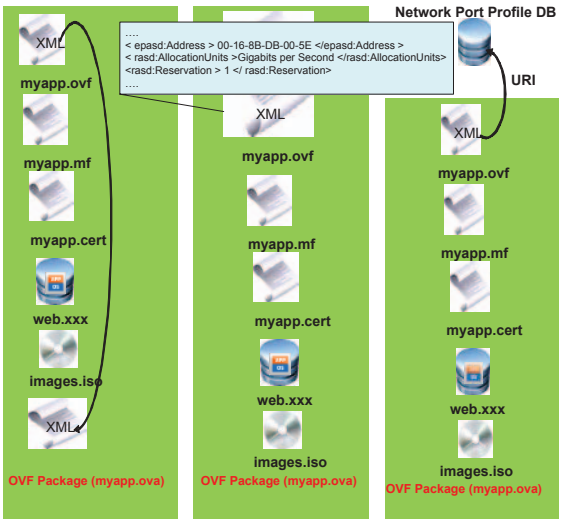


Figure 2 – Network Port Profile Representation Inside an OVF Package

## IV. Network Port Profile Deployment in Pre-Provisioned Network Environments

This section describes a couple of methods for deploying the network port profiles in a pre-provisioned network infrastructure.

### A. Method 1

In this method, the network infrastructure is pre-provisioned with network port profiles. The network administrator pre-provisions the physical network infrastructure based on network port profiles in the network port profile database. Network switches or adjacent switches do not access the network port profile database during the VM deployment. The VM administrator, who is responsible for the OVF packaging and VM deployment/management, understands the network port profile schema and contents. The network port profile information is not contained in the OVF package, and the VM administrator accesses the network port profile database to apply network port profiles to virtual networking components on the virtualization platform during the VM deployment time.

Figure 3 shows the detailed steps involved in applying the network port profiles to the virtual networking components for this method.

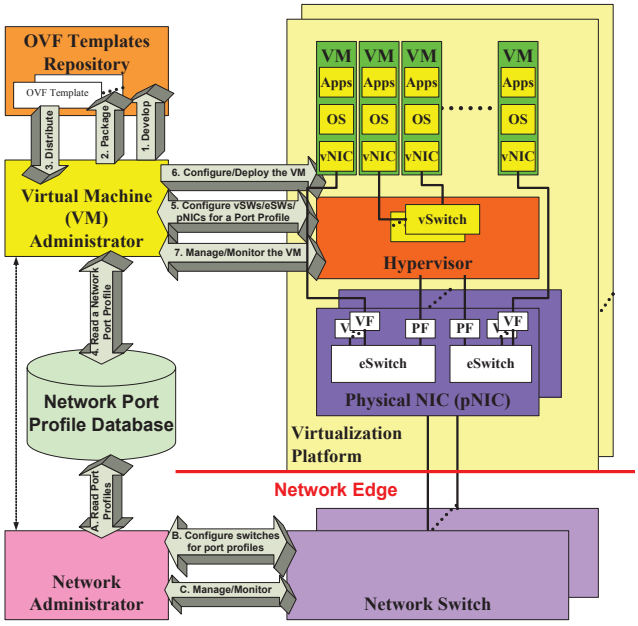


Figure 3 – Network Port Profile Deployment in a Pre-provisioned Network Infrastrucutre (Method 1)

The following describes the flow of steps involved in the provisioning and deployment of virtual networking components from the virtual machine administration side.

*1)* The VM administrator develops, packages, and distributes OVF packages.

*2)* During the deployment of an OVF package, the VM administrator accesses a set of network port profiles that can be applied to the VMs represented in the OVF package.

*3)* Based on the contents of these network port profiles, the VM administrator configures vSwitches, eSwitches, and pNICs of the virtualization platforms on which the VMs are being deployed.

*4)* After that, the VM administrator deploys VMs that connect to the underlying virtual/physical network infrastructures via vNICs that are also configured based on network port profiles.

### B. Method 2

In this method, the network infrastructure is pre-provisioned with network port profiles. The network administrator pre-provisions the physical network infrastructure based on network port profiles in the network port profile database. Network switches or adjacent switches do not access the network port profile database during the VM deployment. The VM administrator, who is responsible for the OVF packaging and VM deployment/management, understands the network port profile schema and contents. The network port profile information is contained in the OVF package to allow the VM administrator to apply network port profile to virtual networking components on the virtualization platform during the VM deployment time. The VM

administrator does not access the network port profile database during the VM deployment.

Figure 4 shows the detailed steps involved in applying the network port profiles to the virtual networking components for this method. The following describes the flow of steps involved in the provisioning and deployment of virtual networking components from the virtual machine administration side.

*1)* The VM administrator develops, packages, and distributes OVF packages. During the packaging of the OVF, the VM administrator incorporates a set of network port profiles in the OVF package.

*2)* During the deployment of an OVF package, the VM administrator uses the network port profile information contained in the OVF package to configure virtual networking components.

*3)* Based on the network port profile information in the OVF package, the VM administrator configures vSwitches, eSwitches, and pNICs of the virtualization platforms on which the VMs are being deployed.

*4)* After that, the VM administrator deploys VMs that connect to the underlying virtual/physical network infrastructures via vNICs that are also configured based on the network port profile contents.

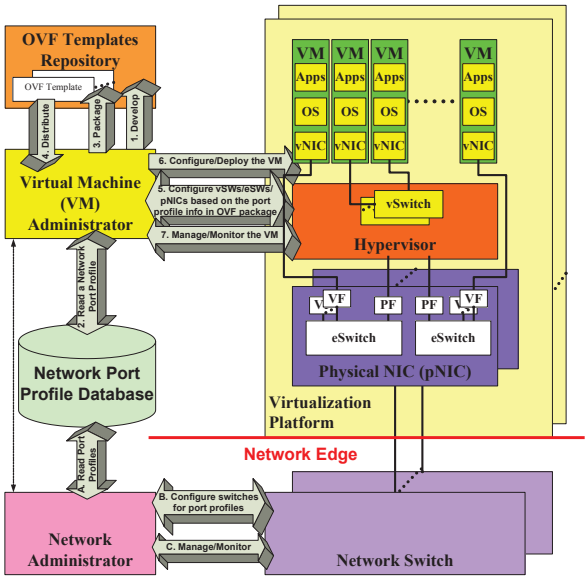


Figure 4 – Network Port Profile Deployment in a Pre-provisioned Network Infrastrucutre (Method 2)

The following are benefits of the methods described in this section:

*1)* These methods enable the deployment of network port profiles on both network infrastructure and virtualization platforms using a common format where the network infrastructure has been pre-provisioned with network port profiles.

*2)* These methods enable static provisioning of network port profiles amd eliminate dynamic association of VMs with the network infrastructure prior to the deployment of network port profiles and VMs on virtualization platforms.

## V. Network Port Profile Deployment in Dynamically Provisioned Network Environments

Network port profiles can be deployed on virtualization platforms in an association-driven dynamically provisioned network infrastructure. In this environment, the network infrastructure is not pre-provisioned with network port profiles. Network switches or adjacent switches access the network port profile database during the VM deployment. The VM administrator, who is responsible for the OVF packaging and VM deployment/management, understands the network port profile schema and contents. The network port profile information is contained in the OVF package to allow the VM administrator to apply network port profile to virtual networking components on the virtualization platform during the VM deployment time. The VM administrator does not access the network port profile database during the VM deployment. The association of VMs with the network infrastructure results in dynamic provisioning and deployment of network port profiles in the network infrastructure.

Figure 5 shows the detailed steps involved in applying the network port profiles to the virtual networking components for this provisioning and deployment method. The following describes the flow of steps involved in the provisioning and deployment of virtual networking components.

*1)* The VM administrator develops, packages, and distributes OVF packages. During the packaging of the OVF, the VM administrator incorporates a set of network port profiles in the OVF package.

*2)* During the deployment of a VM inside the OVF package, the VM administrator initiates a pre-association from the virtualization platform to the underlying network infrastrcuture.

*3)* The virtualization platform requests pre-association with the adjacent bridge. This pre-association request includes the information about the network port profile tied to the the VM being deployed.

*4)* Based on the network port profile information in the pre-association, the adjacent bridge provisions the network infrastructure to support the network port profile. After the network infrastructure has been provisioned, the adjacent bridge responds to the virtualization platform that eventually confirms the pre-association to the VM administrator.

*5)* Based on the pre-association confirmation, the VM administrator configures vSwitches, eSwitches, and pNICs of the virtualization platform on which the VM is being deployed.

*6)* After that, the VM administrator deploys the VM.

*7)* After the VM deployment, the VM is associated and connected with the underlying virtual/physical network infrastructures via vNICs that are also configured based on the network port profile contents.

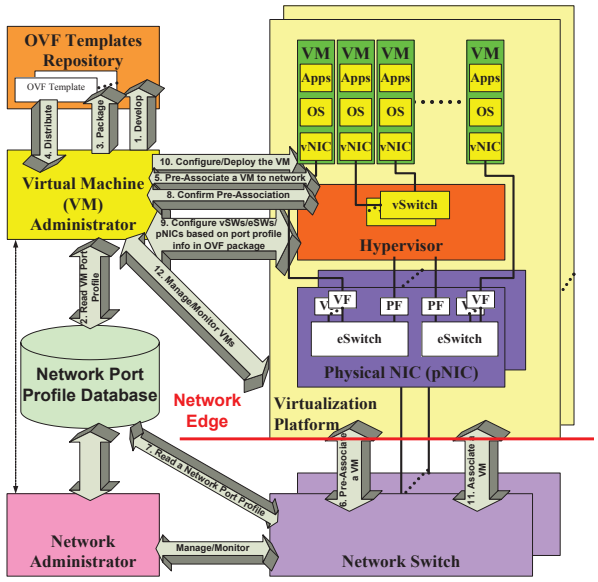


Figure 5 – Network Port Profile Deployment in a Dynamically Provisioned Network Infrastrucutre

The following are the benefits of the method described in this section for deploying network port profiles in a dynamically provisioned network infrastructure:

*1)* It enables the deployment of network port profiles in both network infrastructure and virtualization infrastructure using a common format.

*2)* It allows the deployment of network port profiles without pre-provisioning the network infrastructure. This enables the virtual machines (VMs) to dynamically associate with the network infrastructure and allow the network infrastructure to access network port profiles during the runtime and VM deployment time.

## VI. CONCLUSION

This paper described the network port profile concept, three different ways for incorporating network port profiles in an OVF package, and two models for network port profile-based provisioning and deployment of virtual networking components. The models described in this paper can be used to support standards-based provisioning and deployment of VMs and virtual networking components in a pre-provisioned or dynamically provisioned network environment. In the future, models described in this paper can be extended to incorporate network services such as firewall, load balancing, and QoS into network provisioning and deployment models.

## ACKNOWLEDGMENT

The authors would like to thank all contributors of the network port profile XML Schema and OVF 2.0 standards.

## REFERENCES

[1] DMTF, DSP0243 Open Virtualization Format Specification, Version 2.0, Work-In-Progress, June 2012.

[2] DMTF, DSP2025 Virtual Networking Management White Paper, Version 1.0.0, February 2012.

[3] DMTF, DSP8049 Network Port Profile XML Schema, Version 1.0.0, October 2011.

[4] IEEE, 802.1Qbg, IEEE Standard for Local and Metropolitan Area Networks Amendement---Virtual Bridged Local Area Networks – Amendment: Edge Virtual Bridging.