VMWARE NSX AND OMNISWITCH 6900 INTEROPERABILITY SETUP

APPLICATION NOTE

Alcatel·Lucent Enterprise

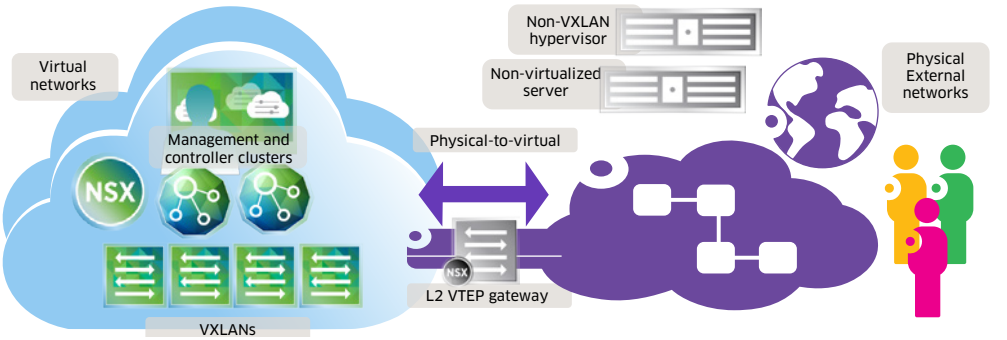
TABLE OF CONTENTS

OVERVIEW

This document describes how Alcatel-Lucent OmniSwitch® 6900 delivers network virtualization services and provides configuration steps to show interoperability with the VMware® NSX™ platform as an L2 hardware virtual extensible local area network (VXLAN) tunnel end-point (VTEP). Figure 1 illustrates the OmniSwitch 6900 bridging virtual network traffic to and from the physical external networks.

The integrated solution of these two platforms meets the technical requirements of today's enterprises using VMware's Software-Defined Data Center (SDDC) principles. This combined solution extends virtualization technologies across the data center and campus infrastructure.

Figure 1: Physical-to-Virtual gateway example



VMware NSX

VMware NSX is the network virtualization platform that creates, deletes and restores software-based virtual networking and the security model from Layer 2 to Layer 7. The NSX platform operates over existing IP networks.

VMware NSX is the "network hypervisor" for hosts virtualizing workloads over VXLANs. Not all hypervisors virtualize over VXLAN and not all servers are virtualized. For this reason it is necessary to allow the bridging and routing of traffic between virtual and physical networks.

OmniSwitch 6900

The OmniSwitch 6900 family supports hardware VTEP, providing the ability to bridge or route traffic to and from external networks or non-VXLAN hypervisors into the VXLAN overlay.

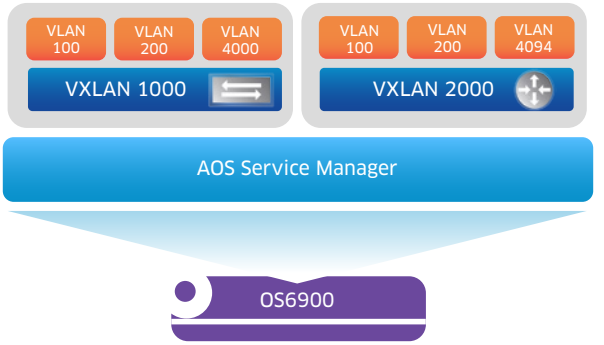
The OmniSwitch 6900 is a key component of our Intelligent Fabric. Intelligent Fabric is an automated network fabric that creates, deletes and restores VLANs and network services. It operates in a programmatic and dynamic fashion enabling IP networking of physical and virtual workloads, which simplifies the tasks of the data center administrator.

The OmniSwitch 6900 offers programmable Shortest Path Bridging Mac-in-mac

(SPB-M) and VXLAN services that deliver departmental segmentation, business unit isolation and transparent subnet extensions over existing enterprise data centers and campus networks.

Figure 2 illustrates how the OmniSwitch extracts network objects to virtualize tenants into containers that offer traffic and control isolation. These containers are administered through the Alcatel-Lucent Operating System (AOS) service manager feature. The AOS Service manager and the Alcatel-Lucent Enterprise Virtual Network Profiles (vNP) technology are the AOS features that deliver network virtualization over SPB-M or VXLAN protocols.

Figure 2: OmniSwitch 6900 network virtualization services

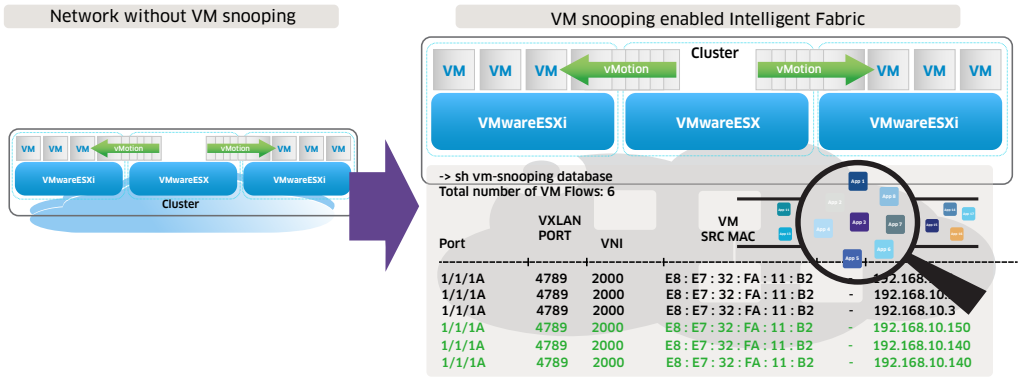


The OmniSwitch 6900 VXLAN services offer the NSX platform a dynamic infrastructure that can be consumed and repurposed on demand using vNP and the OmniSwitch 6900 hybrid-mode hardware VTEP.

The underlying physical infrastructure works as an IP transport to physically interconnect the compute, the management and the controller clusters. The physical infrastructure enabled by Intelligent Fabric offers error-free zero-touch configuration for a flexible and simple network deployment.

Once virtual machine (VM) traffic is encapsulated into VXLAN, the physical network loses visibility to the VM-to-VM communication. To regain visibility and control of the traffic inside the overlay, the VM snooping function must be enabled. VM snooping is unique, and brings a detailed view of the contents of VXLANs and allows for control of the overlay traffic inside the physical network. Vendors without VM snooping capabilities are “blinded” to VXLAN payload information. Figure 3 illustrates VM snooping.

Figure 3: VM snooping



VM snooping allows for discovery of VXLANs and its contents. In addition to discovery, VM snooping also offers dynamic or persistent activation of Access Control List (ACL)/ Quality of Service (QoS) policy list profiles to control VM traffic. The VM traffic can either be discovered, controlled or both by visual network index (VNI), MAC, VLAN, IP, transmission control protocol (TCP)/user datagram protocol (UDP) or a combination of these options. ACL/QoS actions include allow, drop, bandwidth policing, redirection, mirroring, among others. For more information, refer to OmniSwitch user guides.

Alcatel-Lucent OmniVista® 4.1.2.R02 network management software can be used to build the underlying infrastructure and rollout the baseline configuration to prepare the OmniSwitch network for NSX integration. OmniVista then acts as a VMware NSX integration wizard to configure, for example, bidirectional protocol independent multicast routing (PIM-BIDIR), and so on, while the NSX controller orchestrates and manages the VXLANs. OmniVista orchestration is not in the scope of this document.

In this document we will focus on the interoperability of manually configured VXLAN services with NSX software-based virtual networks.

TOPOLOGY

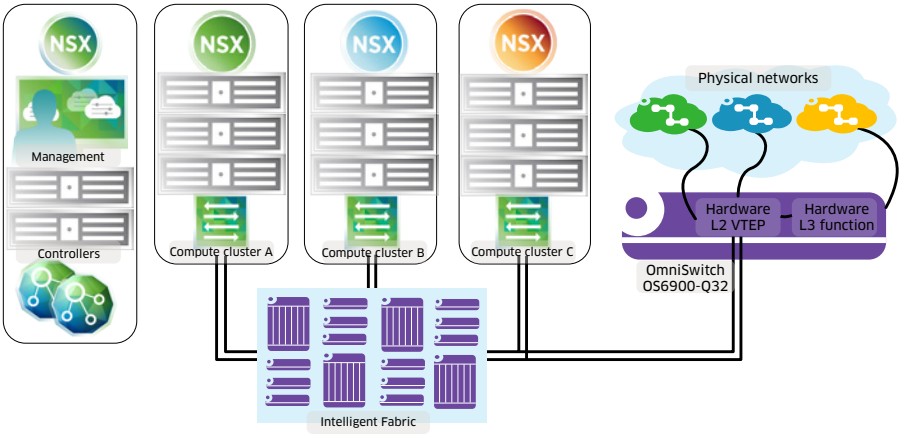
Figure 4 illustrates the following:

1. Ability of the OmniSwitch family to provide the Layer 2 and Layer 3 infrastructure for NSX virtualized networks.

2. Ability of the OmniSwitch family to interoperate with NSX VTEPs to provide Layer 2 and Layer 3 extensions as hardware VTEP.

This topology represents a virtualized data center (DC) with three compute clusters (A, B and C) networked using VMware® NSX Virtual Switches™. The NSX Virtual Switches switch and tunnel data traffic between compute clusters and build the overlay network. The compute clusters are controlled and managed by the NSX controller cluster.

Figure 4: Topology



The NSX controller is the control plane of the NSX infrastructure. It manages the distributed NSX Virtual Switches. The NSX Virtual Switches provide the network forwarding functions to the compute clusters and switch and encapsulate VM traffic into the overlay tunnels. The NSX manager is a web-based graphical user interface used to interact with the NSX controller for configuration of logical switches, tenant networks and VM connectivity. The NSX manager can be supplemented in other environments by cloud orchestrators, such as OpenStack®, to allow workflow provisioning and bulk configurations.

The Intelligent Fabric provides the physical infrastructure to interconnect VMware compute, management and controller clusters. Intelligent Fabric extracts the different components of the network as a single fabric and reduces the complexity of provisioning the access, aggregation and core layers. Intelligent Fabric offers end-to-end connectivity from the overlay network to the physical network end device.

The OmniSwitch 6900-Q32 in this topology operates as a Layer 2 gateway to bridge the logical VXLANs and the physical VLANs in the network. The OmniSwitch 6900-Q32 runs VXLAN as a service to provide hardware-based switching and routing functions for multi-tenant networks and directly attached devices.

COMPONENTS

- 3x VMware vSphere® 6.0
- 1x VMware NSX 6.1.4
- 1x OmniSwitch OS6900-Q32 running AOS 7.3.4.450.R01

OPERATION

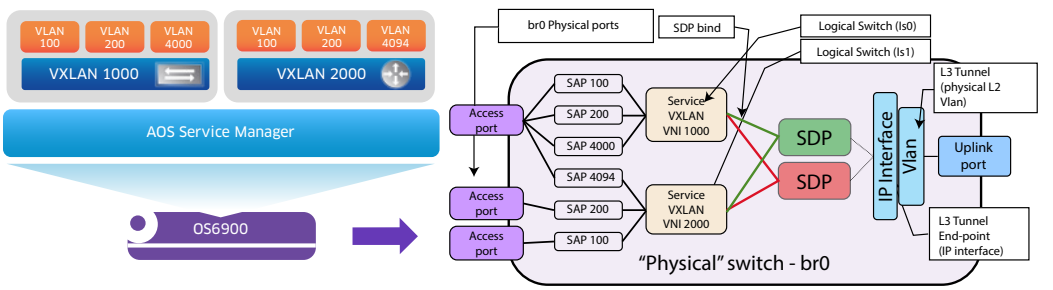
Once the physical infrastructure is prepared for VMware NSX, the NSX orchestration tool discovers and displays the OmniSwitch 6900 as a third-party multicast-enabled VTEP. The OmniSwitch 6900 is registered with NSX to be programmed with the appropriate VXLANs and their associated ports and VLANs. With this setup, VM mobility, learning and connectivity work dynamically without further configuration. OmniVista can also be used to facilitate the preparation of the network.

CONFIGURATION

OmniSwitch 6900

The AOS service manager provides a framework to operate VXLAN or SPB-M technologies as a service in a distributed, multi-tenant network. With service manager VLANs, ports and devices are associated with a VXLAN through the configuration of service objects. This approach defines the VXLAN service domain by configuring the following service components:

Figure 5: Inside AOS service manager



- VXLAN service: The OmniSwitch VTEP identifies each VXLAN segment that the gateway participates in with a VXLAN service ID. A VXLAN service is associated with a VXLAN Network Identifier (VNI) at the time the service is created. The service represents a single virtual bridge or logical switch on the VTEP.

- Access port: An OmniSwitch port or link aggregate can be configured as a service access port. The access port is connected to a host or physical network through which the LAN traffic enters or leaves the VXLAN overlay network. The access port is also associated with a Layer 2 profile that specifies how to process protocol control frames received through the port.

- Service Access Point (SAP): A SAP is a virtual port that binds an access port VLAN(s) to a VXLAN service. It is a virtual port in the logical switch. SAPs can be statically setup through CLI/API or dynamically provisioned through Virtual Network Profiles (vNP). vNP can provide device authentication and classification before the device is accepted into a VXLAN service. vNP can be controlled by a user or device policies administered from a directory manager. Classification rules can include VLANs, MAC addresses, IP addresses or a combination of these. Authentication is executed through IEEE 802.1x providing the most secure multi-tenant cloud data center fabric.

- Service Distribution Point (SDP): An SDP is a logical port that serves as the VXLAN Tunnel Interface (VTI) on a VTEP to extend services to other remote VTEPs. The SDP multiplexes traffic from all associated VXLANs destined to a remote VTEP. An SDP can be configured to transport one or many VXLANs.

- SDP bind: SDP bind represents the binding of a VXLAN service instance to an SDP.

Here is a code configuration snippet that configures an AOS VXLAN service to connect it with NSX Virtual Switches based on manually defined configuration:

```
! SVCMGR:

service vxlan udp-port 8472 « You must change the VXLAN UDP port from its default value (4789, the IANA standard) to 8472 in order to interoperate with NSX.

service access port 1/1/3A « This command defines an access port.

service sdp 10 vxlan multicast-group 239.1.1.1 « This command sets up the tunnel to the remote end points. It accepts unicast or multicast destinations as remote end points.

service 1000 vxlan vnid 1000 « This command creates the VXLAN service instance that corresponds to the logical switch associated with a given VNI.

service 1000 sap port 1/1/3A:100

service 1000 sap port 1/1/3A:200

service 1000 sap port 1/1/3A:4000 « This command creates the service access port association of the virtual port to the logical switch. :x represents a VLAN, all VLANs or untagged VLANs existing in the access port c/s/p.

service 1000 bind-sdp 10 « This command binds the service to a VXLAN tunnel.
```

The above configuration assumes that the Intelligent Fabric provides IP connectivity to all components in the topology shown in Figure 3, including management clusters, controller clusters, compute clusters as well as the designated OmniSwitch VTEP.

To run 'operate in multicast replication' mode, the infrastructure must be running PIM BI-DIR. This document does not provide information on this topic.

The OmniSwitch VTEP can operate in unicast replication mode, multicast replication mode or in hybrid mode. Multicast replication is the default operation and allows for automatic and dynamic discovery of VTEPs. In unicast mode, all remote VTEPs must be explicitly defined. This is an example of a head-end replication configuration:

```
service 2000 vxlan vnid 2000 head-end

service sdp 200 vxlan far-end 10.2.2.2

service 2000 bind-sdp 200
```

SAPs can be created in dynamic fashion using Virtual Network Profiles. This topic is not covered in this document.

VMware NSX

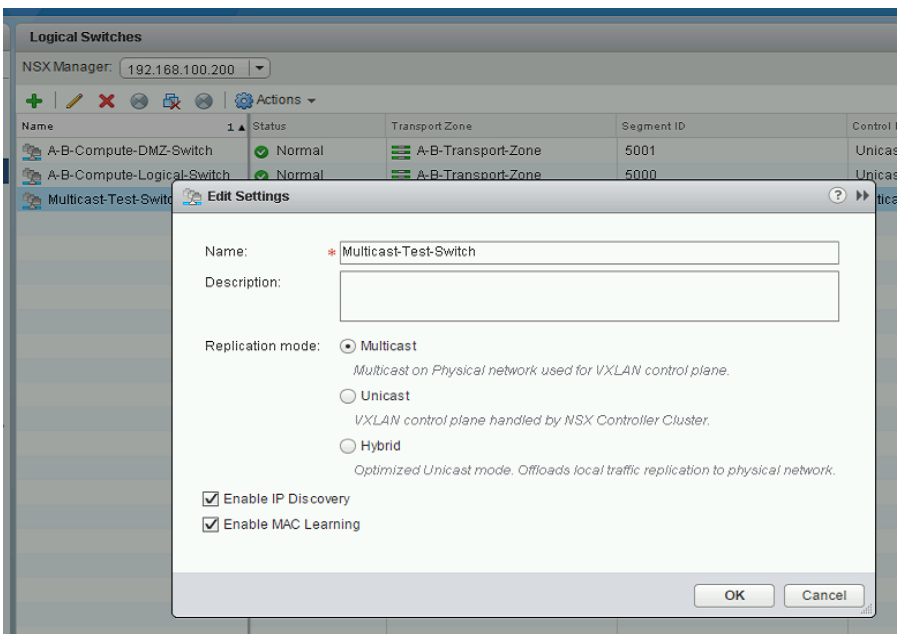
The OmniSwitch must be added to the NSX controller as a logical switch. The steps to include the OmniSwitch in the logical switch list are:

1. Create the OmniSwitch VTEP as a logical switch with replication mode set to multicast (Figure 6).

   Enable IP discovery to allow the VTEP to connect to other VTEPs in the same multicast group.

   Enable MAC learning to use learning functionality in the switch.

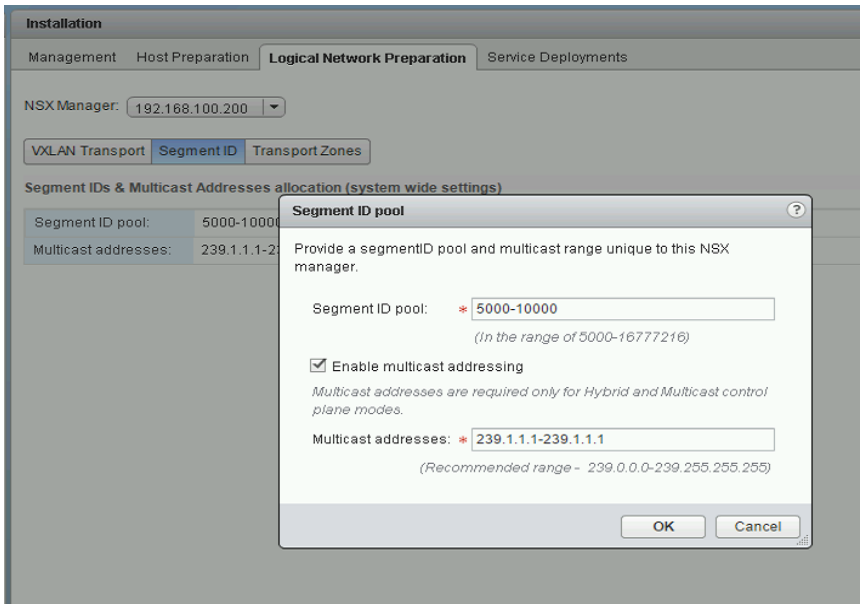
Figure 6: Add OmniSwitch as logical switch



2. Define the multicast group to which the OmniSwitch VTEP should connect to discover other VTEPs.

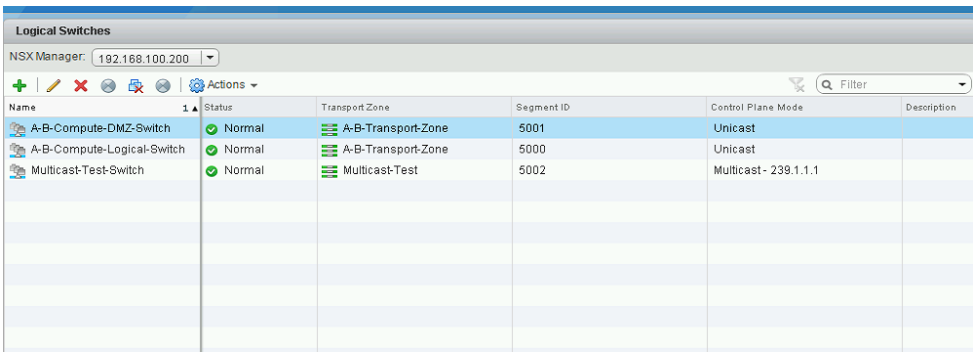
   Configure the VNI range to define the VXLANs available for that VTEP in the specified multicast group. (Figure 7 as a simple test.)

Figure 7: Define VNI range and Multicast group to which the VTEP connects



3. When the configuration is completed and the VTEP is in contact, the OmniSwitch VTEP should be listed as Normal in the Status column. (Figure 8)

Figure 8: Logical switches list



Disclaimer

Alcatel·Lucent Enterprise