Table of Contents

Overview ................................................................. 3
Key VXLAN Components .................................................. 3
   VMware vCloud Networking and Security Manager ......................... 3
   VMware vSphere Distributed Switch ........................................ 3
   Virtual Tunnel End Point ................................................. 4
   VMware vCloud Networking and Security Edge Gateway ................... 4
Example Deployment 1 – Single L2 (One VDS) in a New Deployment ............ 4
   Deployment Components .................................................. 5
   VXLAN Preparation Steps .................................................. 7
      Identify Key Parameters ................................................ 7
      VXLAN Preparation Workflow ......................................... 7
      Virtual Tunnel Endpoint IP Configuration ................................ 11
      Segment ID and Multicast Group Address Range Configuration .......... 14
      Defining VXLAN Network Scope ....................................... 15
      Physical Switch Configuration ........................................ 16
   Consumption of Isolated Logical Networks (Virtual Wires) ................... 17
      Creating Virtual Wire .................................................. 18
      Connecting Virtual Machines to Virtual Wire ............................ 20
      Assigning an IP Address to a Virtual Machine on a Virtual Wire ......... 24
   Deployment and Configuration of vCloud Networking and
   Security Edge Gateway .................................................. 24
      Deploy vCloud Networking and Security Edge Gateway .................. 25
      Configuration of Internal Edge Gateway Interfaces ....................... 34
      Configure Firewall Rule to Allow Access to External Network .......... 41
      Configure Source NAT .................................................. 46
Example Deployment 2 – Multiple L2 (Multiple VDS) – Existing .................... 48
   Deployment Components .................................................. 48
   VXLAN Preparation Steps .................................................. 49
      Identify Key Parameters ................................................ 49
      VXLAN Preparation Workflow ......................................... 49
   Physical Switch Configuration ............................................. 51
   Creation of Virtual Wires ............................................... 53
   Migration of Virtual Machines to Virtual Wires ............................... 53
   Limitation of the Current Deployment Without VXLAN ....................... 55
   Deploy New Web Servers on Cluster 02 ................................... 56
Conclusion ................................................................. 57
About the Author .......................................................... 58
Overview

Organizations worldwide have gained significant efficiency and flexibility in their datacenters as a direct result of deploying VMware® server virtualization solutions. Although compute has been virtualized, network and security technologies in datacenters have struggled to keep pace with the innovations. Many VMware customers are now looking to implement a network virtualization solution that brings flexibility to datacenter networks. Virtual eXtensible Local Area Network (VXLAN), part of VMware vCloud® Networking and Security™, addresses the current networking challenges. This document offers detailed deployment guidelines and step-by-step instructions on how to build VXLAN-based datacenter networks.

A VXLAN-based network virtualization solution addresses the following key challenges that exist in the traditional physical network:

- Limited number of isolated layer 2 (L2) networks (VLAN – 4096)
- Inability to change the physical network configuration on demand
- Limited L2 diameter (because of Spanning Tree Protocol (STP) limitations) that restricts pooling of compute resources available across the datacenter

For more details on the VXLAN-based network virtualization solution and various design consideration details, refer to VMware Network Virtualization Design Guide:

This document is for both vSphere and network administrators. It provides step-by-step configuration instructions for the following two scenarios:

- A brand-new VXLAN network design spanning two compute clusters
- A migration of an existing two-cluster deployment from a standard VLAN to a VXLAN network

Key VXLAN Components

The VMware VXLAN solution consists of the components that follow. They typically are purchased as part of VMware vCloud Suite, which includes VMware vSphere Enterprise Plus Edition™ and VMware vCloud Networking and Security basic licenses.

VMware vCloud Networking and Security Manager

VMware vCloud Networking and Security Manager™ is the centralized network management component of the vCloud Networking and Security product suite. It also has a plug-in to VMware vCenter Server™; users can perform VXLAN configuration through that “network virtualization” plug-in. The plug-in is available only on the VMware vSphere Client™ and is not available on the new, next-generation VMware vSphere Web Client. The Network Virtualization tab appears at the Datacenter object level after vCloud Networking and Security Manager has been configured with the vCenter Server instance IP address and its credentials.

VMware vSphere Distributed Switch

VMware vSphere Distributed Switch™ (VDS) in the vSphere platform provides a single point of management for virtual networking aspects in the datacenter. VDS also provides advanced capabilities, including traffic management, monitoring and troubleshooting features, along with VXLAN support. For more details on the latest VDS features, refer to What’s New in VMware vSphere 5.1 – Networking: http://www.vmware.com/files/pdf/techpaper/Whats-New-VMware-vSphere-51-Network-Technical-Whitepaper.pdf.
Virtual Tunnel End Point

A virtual tunnel endpoint (VTEP) is configured on every host as part of the VXLAN configuration process. The VTEP consists of the following three modules:

1) vmkernel module – VTEP functionality is part of the VDS and is installed as a VMware Installation Bundle (VIB). This module is responsible for VXLAN data path processing, which includes maintenance of forwarding tables and encapsulation and deencapsulation of packets.

2) vmknic virtual adapter – This adapter is used to carry VXLAN control traffic, which includes response to multicast join, DHCP, and ARP requests.

3) VXLAN port group – This is configured during the initial VXLAN configuration process; includes physical NICs, VLAN information, teaming policy, and so on. These port group parameters dictate how VXLAN traffic is carried in and out of the host VTEP through the physical NICs.

Each vSphere host VTEP is assigned with a unique IP address, which is configured on the vmknic virtual adapter and is used to establish host-to-host communication tunnels and carry VXLAN traffic.

VMware vCloud Networking and Security Edge Gateway

The VMware vCloud Networking and Security Edge™ gateway is a virtual appliance with advanced network services support such as perimeter firewall, DHCP, NAT, VPN, load balancer, and VXLAN gateway function.

The VXLAN gateway function of the vCloud Networking and Security Edge gateway is one of the key components of the VXLAN network design. The vCloud Networking and Security Edge gateway acts as a transparent bridge between the VXLAN and non-VXLAN infrastructure. It is used in the following scenarios:

1) When a virtual machine connected to a logical L2 network must communicate with a physical server or virtual machine running on a host that does not support VXLAN, the traffic is directed through the vCloud Networking and Security Edge gateway.

2) When a virtual machine on one logical L2 network must communicate with a virtual machine on another logical L2 network, the vCloud Networking and Security Edge gateway can provide that connectivity.

The vCloud Networking and Security Edge gateway is a highly available virtual appliance that is deployed in an active–standby configuration and has as many as 10 interfaces. It is offered in three sizes: compact, full and x-large. Users have the option of scaling up their vCloud Networking and Security Edge gateway design by increasing the size of the appliance or of scaling out by using multiple virtual appliances.

Example Deployment 1 – Single L2 (One VDS) in a New Deployment

In this example, we configure VXLAN and then deploy a three-tier application. During the application deployment process, we show how to create logical L2 networks—also known as virtual wires—and how to connect the application’s virtual machines to these virtual wires. Finally, we configure a vCloud Networking and Security Edge gateway to provide access from the isolated logical L2 network to the external world. You can choose to configure other network services such as firewall, load balancer, VPN, and DHCP server on the vCloud Networking and Security Edge gateway.
Deployment Components

The following components are used in this deployment:

- Two clusters in the same vCenter datacenter
  - Two hosts per cluster
  - Two 10GbE network interface cards per host
- Two physical switches
- One VDS
- Management cluster
  - vCenter Server
  - vCloud Networking and Security Manager

To install each component in your environment, refer to the respective installation guide.

Figure 1 shows the initial deployment, before the VXLAN-based network virtualization solution is configured. The two clusters are hosted on two different racks in the datacenter. For the new deployment, follow these recommendations regarding configuration of the physical network infrastructure:

- Configure one VLAN between the two clusters for carrying the VXLAN transport traffic. By provisioning one VLAN for transport, the requirement to enable multicast routing on the physical switches is eliminated.
- Configure IGMP snooping and IGMP querier functions on the physical switches.

In this setup, VLAN 2000 is configured on the physical switches to carry the VXLAN traffic. The other infrastructure VLANs for VMware vSphere vMotion®, management and NFS traffic typically used in a vSphere deployment are not shown in this diagram but are assumed to be present.

The vSphere Client screenshot in Figure 2 shows the component inventory under the vCenter Server instance managing the two clusters in a datacenter VXLAN-DC.
Figure 2. Hosts and Clusters View

Figure 3 shows the VXLAN-VDS network configuration with two uplinks. All four hosts are part of this VDS.

Figure 3. Network View
VXLAN Preparation Steps

Identify Key Parameters
The following parameters are used during the VXLAN configuration preparation workflow:

- Name of the VDS where you want to deploy VXLAN VIB—in this example, VXLAN-VDS.
- VLAN ID over which all the VXLAN traffic will be carried: VLAN 2000.
- Teaming algorithm is configured or not configured on the physical switch ports; in this example, no teaming is configured. Use Explicit failover as the teaming configuration on the port group defined for the VXLAN traffic.
- DHCP service in VLAN 2000 subnet is available or not available; in this example, no DHCP service is available.

VXLAN Preparation Workflow
First, select the VXLAN-DC datacenter on the left panel. Then, click Network Virtualization on the right panel as shown in Figure 4:

![Figure 4. Network Virtualization – vCloud Networking and Security Manager Plug-in](image)

Under Network Virtualization, click Preparation to start the VXLAN configuration process.

![Figure 5. VXLAN Preparation](image)
After clicking **Preparation**, click **Edit**.

![Figure 6. VXLAN Configuration – Connectivity](image)

The following screenshot contains the option to choose the number of clusters over which the VXLAN fabric must be prepared. In this setup, there are two clusters configured. Those clusters are shown in Figure 7.

![Figure 7. VXLAN Configuration – Connectivity – Select Clusters](image)

After selecting the clusters, choose the distributed switch for both clusters and then configure VXLAN transport VLAN 2000. In this deployment VXLAN-VDS is used across both the clusters.
Provide the VXLAN transport VLAN ID 2000 in the VLAN field as shown in Figure 9 and click **Next**.
Next, select the teaming configuration that will be used on the VXLAN transport port group and the MTU size. In this example, no teaming is configured on the physical switches, so use **Fail Over** teaming and keep the 1600 bytes default MTU.

![Figure 10. VXLAN Configuration - Connectivity - Select Teaming](image)

After you click **Finish**, vCloud Networking and Security Manager enables the VXLAN module on each vSphere host. It also configures the vmknic and port groups as part of the VTEP preparation. The screenshot in Figure 11 shows the status after completion of the VTEP configuration process.

![Figure 11. VXLAN Configuration - Connectivity - Finish](image)
Figure 12 shows the various components that vCloud Networking and Security Manager installs on each host.

Virtual Tunnel Endpoint IP Configuration

The IP configuration for each VTEP can be performed automatically through a DHCP server infrastructure. In this example, the DHCP server is not present, so manual IP configuration steps are provided.

This configuration involves selecting each host and modifying the virtual adapter property. As shown in Figure 13, first select a host; then select the networking configuration, to change the parameters of the virtual adapter.
Edit the properties of the vmknic that was created during the previous VXLAN preparation workflow. Then assign the IP in the subnet that is mapped to VLAN 2000.

Figure 14. Manual VTEP Configuration – Edit VXLAN vmknic (vmk2)
Figure 15. Manual VTEP Configuration – Assign Static IP

The screenshot in Figure 16 provides the details of each VTEP IP following the manual changes to the IP addresses across all four hosts in the cluster. The next step configures segment ID and multicast group address configurations. Click Segment ID.
Figure 16. Manual VTEP Configuration – Repeat for All Hosts – VXLAN vmknic

Segment ID and Multicast Group Address Range Configuration

Check with your network administrators to determine which multicast group address range you can configure. Also identify the number of isolated logical L2 networks you want to create. In this example, 2,000 logical L2 networks are possible with the segment ID of 5000 to 7000.
In the **Multicast addresses** field, provide the multicast address range that will be used to associate with the segment IDs. One-to-one mapping between segment ID and multicast group address is recommended.

As a best practice, it is important to work with the networking team to identify a range of multicast addresses that can be used in your environment for the VXLAN deployment. The following are some of the key points to remember:

1) Do not use multicast addresses ranging from 224.0.0.1 to 224.0.0.255. These are reserved for routing protocols and other low-level topology discovery or maintenance protocols.

2) Out of the remaining groups ranging from 224.0.1.0 to 239.255.255.255, use administratively scoped addresses from 239.0.0.0 to 239.255.255.255 if the VXLAN deployment is within a company. This multicast address range is viewed as a private multicast domain similar to the 10.0.0.0/8 range, so it is not used for global Internet traffic.

3) In some deployments where VXLAN networks will be shared between administrative domains, the addresses should be assigned from the 232.0.0.0/8 (232.0.0.0-232.255.255.255) source-specific block.

**Defining VXLAN Network Scope**

The network scope defines the range of the logical networks. In this example, the VXLAN-based logical network range is configured to span both compute clusters. As shown in Figure 19, click **Network Scopes** and then the “+” icon to define a new network scope.
Enter the name of the network scope and then select both clusters to be part of the VXLAN-Fabric-Scope.

Through these configuration steps, you have the option to increase or decrease the scope of the network. Follow the previously described steps when you want to add or remove compute clusters to or from the network scope.

Physical Switch Configuration
In this example, the following configurations are required on the physical switches:

1) Configure VLAN 2000 on both switches.
   a. Switch ports facing vSphere hosts are configured as trunk with VLAN 2000 and other infrastructure VLANs configured.
   b. The port channel between the two switches also carries VLAN 2000.
2) Configure IGMP snooping.
3) Enable IGMP querier on VLAN 2000.
4) Increase MTU size to 9,216. There are two options available: Either globally change the MTU size across all switch ports or perform per-port changes.

Switch 1 Configuration

1) VXLAN VLAN configuration

Switch-Router1# interface vlan 2000
Switch-Router1 (config-if)# ip address 172.168.10.1 255.255.255.0
Switch-Router1 (config-if)# no shutdown
Switch-Router1 (config-if)# end
2) IGMP snooping configuration
Switch-Router1 (config)# ip igmp snooping
Switch-Router1 (config)# end

3) IGMP querier configuration
Switch-Router1# interface vlan 2000
Switch-Router1 (config-if)# ip igmp snooping querier
Switch-Router1 (config-if)# end

4) MTU configuration (shown only for one port)
Switch-Router1# interface gigabitEthernet 4/1
Switch-Router1 (config-if)# mtu 9216
Switch-Router1 (config-if)# end

Switch 2 Configuration

1) VXLAN VLAN configuration
Switch-Router2# interface vlan 2000
Switch-Router2 (config-if)# ip address 172.168.10.2 255.255.255.0
Switch-Router2 (config-if)# no shutdown
Switch-Router2 (config-if)# end

2) IGMP snooping configuration (global)
Switch-Router2 (config)# ip igmp snooping
Switch-Router2 (config)# end

3) IGMP querier configuration
Switch-Router2# interface vlan 2000
Switch-Router2 (config-if)# ip igmp snooping querier
Switch-Router2 (config-if)# end

4) MTU configuration (shown only for one port)
Switch-Router2# interface gigabitEthernet 4/1
Switch-Router2 (config-if)# mtu 9216
Switch-Router2 (config-if)# end

Consumption of Isolated Logical Networks (Virtual Wires)
After the VXLAN fabric has been created, you can consume the isolated logical L2 networks on demand. In this section, we will create three different logical networks for the three virtual machines of a three-tier application. We will look at the following steps in the logical network consumption process:

1) Creating virtual wire
2) Connecting virtual machines to virtual wire
3) Assigning an IP address to the virtual machines on the virtual wire
**Creating Virtual Wire**

To create a new logical network, first click **Networks**, as shown in Figure 22. Then click the “+” icon.

![Figure 22. VXLAN Virtual Wire – Click Networks](image)

![Figure 23. VXLAN Virtual Wire – Add](image)
Then define the name of the virtual wire. After clicking **Ok**, you will see that a logical network is created with segment **ID 5000** and associated multicast group address **225.1.1.1**.

Repeat the previous steps and create two more virtual wires for the application and database server virtual machines.
Connecting Virtual Machines to Virtual Wire
There are two methods of connecting a virtual machine to a virtual wire:

1) Using vCloud Networking and Security Manager
2) Editing the virtual machine setting and changing the port group assignment

Option 1: vCloud Networking and Security Manager
In this option, first select the virtual wire on which you want to connect a virtual machine.
After clicking the "+" icon, search for the name of the virtual machine, as shown in Figure 30.

Select the virtual machine and then click **Next**. As shown in Figure 31, the process of connecting the Web server virtual machine is complete.
Option 2: Edit Virtual Machine Setting and Port Group Choice

Instead of using vCloud Networking and Security Manager in this option, you can change the connection of a virtual machine by editing the settings of the network adapter.

Each virtual wire created in a VXLAN environment is associated with a port group on the distributed switch. In Figure 32, there are three port groups and three virtual wires: Web, application and database.

In the Hosts and Clusters view, select the Application Server virtual machine and then click Edit Settings.
From the drop-down menu, select the **Application Virtual Wire** port group for this application server virtual machine.
Figure 35 shows the three-tier application virtual machines connected to the three virtual wires.

Assigning an IP Address to a Virtual Machine on a Virtual Wire

You can choose to either manually assign static IP addresses to virtual machines connected to different virtual wires or make use of the vCloud Networking and Security Edge gateway DHCP service and assign them automatically. In this example, we assigned the following subnets to the three virtual wires and configured static IP addresses from the respective subnets to the virtual machines:

1) Web virtual wire – 192.168.10.0/24
2) Application virtual wire – 192.168.20.0/24
3) Database virtual wire – 192.168.30.0/24

The three virtual machines connected to the virtual wires are isolated from each other. To provide communication between the various tiers of application, or communication with the external world, vCloud Networking and Security Edge gateway must be deployed.

Deployment and Configuration of vCloud Networking and Security Edge Gateway

The vCloud Networking and Security Edge gateway acts as a VXLAN gateway along with other functions such as firewall, load balancer, VPN, DHCP services, and so on. This section covers the deployment of a vCloud Networking and Security Edge gateway and provides steps to enable access to the external network from the internal virtual wires. The following are some of the key deployment and configuration steps covered as part of the vCloud Networking and Security Edge gateway installation.

1) Deploy vCloud Networking and Security Edge gateway.
2) Connect virtual wires to the vCloud Networking and Security Edge gateway.
3) Configure firewall rule for external access.
4) Configure NAT.
Deploy vCloud Networking and Security Edge Gateway

To deploy a vCloud Networking and Security Edge gateway virtual appliance, click **Edges** and then click the "+" icon.

![Figure 36. Deploy vCloud Networking and Security Edge – Add](image)

To provide reliability to the vCloud Networking and Security Edge gateway functions, click **Enable HA**.

![Figure 37. Deploy Edge – Enable HA](image)
There are three size options to choose from while deploying the vCloud Networking and Security Edge gateway appliance. You also can provision the appliance in a particular cluster or on a vSphere host.
Figure 39. Deploy vCloud Networking and Security Edge Gateway – Choose Appliance Size
In this example, we choose the compact size for the vCloud Networking and Security Edge appliance and provision it on Host 05 of Cluster 01.
Next we will configure the interfaces of the vCloud Networking and Security Edge gateway appliance. As part of this interface configuration, we select the external interface first, to configure its properties; then, we configure the internal interfaces, where the three virtual wires or VXLAN logical L2 networks will be connected.
Figure 42. Deploy vCloud Networking and Security Edge - Interface Configuration
Click Select. A pop-up window provides three options for connecting the external vCloud Networking and Security Edge gateway interface:

1) Virtual wire – Enables you to connect to VXLAN-based logical L2 networks.
2) Standard port group – Provides the option to connect to a port group on a standard switch. In this example, we don’t have any standard switch in the deployment.
3) Distributed port group – Enables you to connect to a port group created on the VDS. In this deployment, we choose this option and connect the external interface of the vCloud Networking and Security Edge gateway to the External-Access port group.
After selecting the external interface network connection, assign the IP address for that external interface of the vCloud Networking and Security Edge gateway.
Figure 45. Deploy vCloud Networking and Security Edge – Assign External IP
After configuring the external interface, we configure the three internal interfaces on the vCloud Networking and Security Edge appliance. These internal interfaces connect to the internal virtual wires.

**Configuration of Internal Edge Gateway Interfaces**

As shown in Figure 47, a new interface, **Web Server Gateway Interface**, is created on the vCloud Networking and Security Edge gateway. The interface is connected to a Web virtual wire, and an IP address is assigned. Repeat these steps for the other two virtual wires by creating two more vCloud Networking and Security Edge interfaces.
Click Select. A pop-up window provides three options for connecting the internal vCloud Networking and Security Edge gateway interface. We select **Virtual Wire**, which enables us to connect to one of the VXLAN-based logical L2 networks.
Figure 48. Deploy vCloud Networking and Security Edge – Connect to Web Virtual Wire

Figure 49. Deploy vCloud Networking and Security Edge – Assign IP Address
After the interface configuration, we configure the default gateway for the external interface. In this example, the default gateway is the VLAN 2000 interface IP address configured on the physical switch. However, if a VRRP or HSRP configuration exists at the routing layer, consult with the network team and get the default gateway IP address.
After the gateway IP address configuration, we have the option of defining the management IP address for VMware vSphere High Availability (HA) communication between vCloud Networking and Security Edge gateways. In this example, the platform selects the IP address for HA communication.
Figure 52. Deploy vCloud Networking and Security Edge - VMware vSphere High Availability
Figure 53. Deploy vCloud Networking and Security Edge - Configuration Summary

This concludes the configuration of the vCloud Networking and Security Edge gateway interfaces.
Figure 54. Deploy vCloud Networking and Security Edge – In Active Standby

Figure 55 shows the various interface connections of the vCloud Networking and Security Edge active and standby appliances in Cluster 01 after the deployment and configuration process. As shown in the diagram, the external interface of the vCloud Networking and Security Edge gateway is connected to the green external PG configured with VLAN 100; internal interfaces are connected to the virtual wire port groups.

Configure Firewall Rule to Allow Access to External Network

The vCloud Networking and Security Edge gateway also acts as a perimeter firewall. You can configure the firewall to allow the devices connected on the internal networks to have external access.
In this example, we provide access to the internal Web server virtual machines and allow them to connect to the external network. The screenshot in Figure 58 shows the various interfaces on the vCloud Networking and Security Edge gateway appliance.
As shown in Figure 59, by default, the firewall rule denies all traffic from any source to any destination.

We will now create a rule to allow traffic from the Web server gateway interface (source) to the external interface (destination) of the vCloud Networking and Security Edge gateway.
As shown in Figure 61, you can create a firewall rule based either on IP addresses or on VnicGroup. The VnicGroups are the interfaces of the vCloud Networking and Security Edge gateway. To apply firewall rules to all virtual machines connected on a particular interface, the VnicGroup option is better.

In this example, to allow traffic from all the Web servers to the external world, choose the VnicGroup-based firewall rule. Then select `vnic-index-1`, which associates with the Web server gateway interface as the source of the traffic.
After selecting the source VnicGroup, select the external interface as the destination of the traffic.

The source and destination fields of the firewall rules have been configured. Now select the type of service you want to enable or disable as part of this rule. As shown in Figure 64, any service from Web servers is allowed to the external world.

Finally, publish the firewall rule.
Configure Source NAT

The configuration of NAT is required in this scenario because the internal Web server IP addresses are assigned in the private IP space 192.168.10.0/24. The external network is configured as 172.168.10.0/24. In Figure 65, the blue virtual wire in the top left corner shows the connection between the two Web servers on the 192.168.10.0/24 network.

![Figure 65. IP Address Configuration – Various Virtual Wires and the External Network](image)

The following screenshots walk you through the steps of configuring the SNAT rule for the Web servers:

![Figure 66. vCloud Networking and Security Edge Configuration – NAT Rule](image)
Figure 67. vCloud Networking and Security Edge Configuration – Add SNAT Rule to Provide External Access to the Web Server Virtual Machine

Figure 68. vCloud Networking and Security Edge Configuration – Apply NAT Policy on the External Interface
This example deployment provides a guideline on how to enable VXLAN and configure some of the features of the vCloud Networking and Security Edge gateway. For details on configuring the other features of vCloud Networking and Security Edge gateway, refer to vCloud Networking and Security user-guide documents.

**Example Deployment 2 – Multiple L2 (Multiple VDS) – Existing**

After having gone through a brand-new deployment, in this section we examine an existing two-cluster deployment that utilizes a traditional VLAN-based network configuration and how to transition it to a VXLAN-based network. During this exercise, we also migrate the existing three-tier application’s virtual machines from standard port groups to VXLAN virtual wires.

**Deployment Components**

The various components used in this deployment, shown in Figure 70, are as follows:

- Two clusters
  - Two hosts per cluster
  - Hosts with two 10GbE network interface cards
  - Two separate VDSs (one per cluster)
- Virtual network configuration per VDS
  - vMotion port group (not shown)
  - NFS port group (not shown)
  - Management port group (not shown)
- Virtual machine port groups – Web server, application server and database server port groups on VDS01.
  - Port group X, port group Y and port group Z on VDS02
• Two physical switches with routing capability
  • Routing enabled between VLANs
• Management cluster
  • vCenter Server
  • vCloud Networking and Security Manager

Figure 70. Existing Deployment – Two-Cluster Design with a Three-Tier Application Running

VXLAN Preparation Steps
In this section, we go through the steps of configuring VXLAN on top of an existing two-cluster deployment with a three-tier application running.

Identify Key Parameters
Before starting the configuration process, make note of the following parameters in your environment. These parameters will be used during the VXLAN preparation workflow:

• Number of clusters in your setup – Two: Cluster 01 and Cluster 02
• Number of VDSs – Two: “Cluster01-VXLAN-VDS” and “Cluster02-VXLAN-VDS”
• Number of port groups per VDS for virtual machine traffic – Three port groups with three different VLANs. The VLANs that are used to isolate various virtual machine traffic are not required after VXLAN is deployed.
• From the available virtual machine port groups, select a VLAN for VXLAN transport traffic. For example, select one of the virtual machine–traffic VLANs in each cluster as the VXLAN transport VLAN: “VLAN 2000,” “VLAN 2010.”
• Teaming algorithm configured on the physical switch ports or not – No teaming configured. Use “Explicit failover” as the teaming configuration on the port group defined for the VXLAN transport traffic.

VXLAN Preparation Workflow
The workflow is very similar to the one described in example deployment 1. The only difference is in the parameters configured during the workflow. Different VDSs are selected, and two different VLANs are configured as VXLAN transport VLANs, as shown in Figure 71.
**Figure 71.** VXLAN Preparation Workflow – VDS and VLAN

**Figure 72.** VXLAN Preparation Workflow – Teaming
Physical Switch Configuration

In this example, the following configurations are required on the physical switches:

1) Configure VLAN 2000 on Switch 1 and VLAN 2010 on Switch 2 to carry the VXLAN traffic. You can also decide to reuse one of the existing VLANs for this purpose.
   a. Switch ports facing vSphere hosts are configured as trunks. These trunk ports allow VLAN 2000/2010 and other infrastructure VLANs.
   b. The port channel between the two switches also carries VLAN 2000/2010.
2) Configure snooping.
3) Enable multicast routing.
4) Configure rendezvous point on Switch-Router 1 for PIM-Sparse mode.
5) Enable PIM-Sparse mode.
6) Increase MTU size to 9,216.

The following are the switch command details:

**Switch 1 Configuration**

1) VXLAN VLAN configuration

Switch-Router1# interface vlan 2000
Switch-Router1 (config-if)# ip address 172.168.10.1 255.255.255.0
Switch-Router1 (config-if)# no shutdown
Switch-Router1 (config-if)# end

2) IGMP snooping configuration

Switch-Router1 (config)# ip igmp snooping
Switch-Router1 (config)# end

3) Enable multicast routing

Switch-Router1 (config)# ip multicast-routing
Switch-Router1 (config)# end

4) Configure RP (rendezvous point)

Switch-Router1 (config)# ip pim rp-address 172.168.10.1
Switch-Router1 (config)# end

5) Enable PIM-Sparse-dense-mode

Switch-Router1# interface vlan 2000
Switch-Router1 (config-if)# ip pim sparse-mode
Switch-Router1 (config-if)# end

6) MTU configuration (shown for only one port)

Switch-Router1# interface gigabitEthernet 4/1
Switch-Router1 (config-if)# mtu 9216
Switch-Router1 (config-if)# end

**Switch 2 Configuration**

1) VXLAN VLAN configuration

   a. Switch-Router1# interface vlan 2010
   b. Switch-Router1 (config-if)# ip address 172.168.20.1 255.255.255.0
   c. Switch-Router1 (config-if)# no shutdown
   d. Switch-Router1 (config-if)# end

2) IGMP snooping configuration

   a. Switch-Router1 (config)# ip igmp snooping
   b. Switch-Router1 (config)# end

3) Enable multicast routing

   a. Switch-Router1 (config)# ip multicast-routing
   b. Switch-Router1 (config)# end
4) Configure RP (rendezvous point)
   a. Switch-Router1 (config)# ip pim rp-address 172.168.10.1
   b. Switch-Router1 (config)# end

5) Enable PIM-Sparse-dense-mode
   a. Switch-Router1# interface vlan 2010
   b. Switch-Router1 (config-if)# ip pim sparse-mode
   c. Switch-Router1 (config-if)# end

6) MTU configuration (shown for only one port)
   a. Switch-Router1# interface gigabitEthernet 4/1
   b. Switch-Router1 (config-if)# mtu 9216
   c. Switch-Router1 (config-if)# end

Creation of Virtual Wires

The steps for creating virtual wires are the same as those described in the “Consumption of Virtual Wire” section in example deployment 1. The screenshot in Figure 75 shows the three virtual wires created for the three-tier application.

![Figure 75. VXLAN Virtual Wire Creation – Create Three Virtual Wires](image)

Migration of Virtual Machines to Virtual Wires

After creating the various virtual wires for the three-tier application, we can migrate the virtual machines connected from the standard port groups, with VLANs, to the virtual wires. There are two options for migrating as described in example deployment 1; refer to the “Connecting Virtual Machines to Virtual Wire” section for step-by-step instructions.

The following screenshots provide the steps of migrating two Web servers to the Web virtual wire.
Figure 76. Migration of Virtual Machine to Virtual Wires – Web Servers

Figure 77. Migration of Virtual Machine to Virtual Wires – Moved from Standard Port Group to Virtual Wire
Limitation of the Current Deployment Without VXLAN

In the current deployment, as shown in Figure 78, the three-tier application utilizes compute resources from only Cluster 01; Cluster 02 resources are not used because the L2 adjacency requirements for the application are not met by Cluster 02, which is configured in a different VLAN. As shown in Figure 70, Cluster 01 is backed by VLAN 2000, 2001, 2002; Cluster 02 is backed by VLAN 2010, 2011, 2012.

This challenge/limitation is addressed with VXLAN virtual wires. Users now can efficiently use the resources available across the datacenter. As shown in Figure 80, the virtual wires span across the two clusters, and virtual machines connected to these virtual wires perform as if they were connected to the same L2 network. Currently, there are two Web server virtual machines connected to the Web virtual wire, as indicated by the red rectangle. These Web servers are deployed on Cluster 01.
If the demand for application grows and there is a need to provision an additional two Web servers, users can utilize the compute resources in Cluster 02 and connect the virtual machines to the Web server virtual wire.

### Deploy New Web Servers on Cluster 02

The screenshot in Figure 81 shows the additional virtual machines connected to the Web virtual wire.
These Web servers can be load balanced using the vCloud Networking and Security Edge gateway Load Balance feature. Also, as described in example deployment 1, users can utilize the firewall capability and provide security between different tiers of application. For more details on how to use the vCloud Networking and Security Edge gateway feature, refer to the vCloud Networking and Security Edge gateway configuration documents.

**Conclusion**

The network virtualization solution using VXLAN technology provides flexibility and agility in provisioning diverse workloads across the various racks of compute resources in a datacenter. This is achieved by creating an overlay network on top of the existing datacenter network. Users now can create logical networks on demand and consume those networks without requiring changes to any of the physical network configurations.
About the Author

Vyenkatesh (Venky) Deshpande is senior technical marketing manager in the Technical Marketing group at VMware, with a technology focus on networking. He has worked in the networking industry for more than 15 years and has been with VMware since August 2010. His responsibilities include vSphere networking-features collateral and the vCloud Networking and Security suite of products.

Follow Venky’s blog at http://blogs.vmware.com/vsphere/networking

Follow Venky on Twitter @VMWnetworking