Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV2(2.1a)

First Published: October 15, 2013

Last Modified: March 15, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-30691-01

CONTENTS

Preface

Preface vii

Audience vii

Document Conventions vii

Related Documentation for Nexus 1000V Series NX-OS Software for VMware vSphere ix

Documentation Feedback x

Obtaining Documentation and Submitting a Service Request x

CHAPTER 1

Overview 1

Information About VXLANs 1

Overview of VXLANs 1

VXLAN Tunnel Endpoints 3

VXLAN Gateway 3

VXLAN Trunks 4

Multi-MAC Capability 4

Fragmentation 4

Scalability 4

Maximum Number of VXLANs 4

Supported Features 5

Jumbo Frames 5

VXLAN Feature Disabled 5

VXLAN Offload 5

CHAPTER 2

Configuring VXLANs 7

Information About VXLANs 7

Prerequisites for VXLANs 7

Guidelines and Limitations for VXLANs 8

Default Settings for VXLANs 9

Configuring VXLANs 9
Initial Enabling of VXLANs 9
Enabling VXLANs 9
Configuring vmknics for VXLAN Encapsulation 10
Creating a Bridge Domain 12
Configuring the Bridge Domain Mode 13
Creating a Port Profile Configured to Use a VXLAN 14
Removing Ports from a VXLAN 16
Deleting a VXLAN 17
Disabling Segmentation 17
Verifying the VXLAN Configuration 19
Feature History for VXLAN 20

CHAPTER 3 **Installing and Configuring VXLAN Gateway 21**
Information About the VXLAN Gateway Deployment 21
Guidelines and Limitations 22
Configuring VSMs 23
Configuring VXLAN Termination/VTEP on the VXLAN Gateway 25
Installing a VXLAN Gateway as a Virtual Service Blade 27
Setup Script to Configure the VXLAN Gateway 28
Modifying the Initial Setup Script Parameters 30
Configuring High Availability 31
32
Verifying the VXLAN Gateway Installation and Configuration 32
Managing the VXLAN to VLAN Mappings on the VXLAN Gateway 38
Deleting the VXLAN Gateway 39
39
Feature History for VXLAN Gateways 40

CHAPTER 4 **Configuring Advanced Features 41**
Configuring VXLAN Trunks 41
Configuring Multi-MAC Capability 42

CHAPTER 5 **Upgrading VXLAN Gateway from VSM 45**
Upgrading VXLAN Gateway Service Module 45

Upgrading VXLAN Gateway Cluster 46

Preface

This preface contains the following sections:

- Audience, page vii
- Document Conventions, page vii
- Related Documentation for Nexus 1000V Series NX-OS Software for VMware vSphere, page ix
- Documentation Feedback, page x
- Obtaining Documentation and Submitting a Service Request, page x

Audience

This publication is for experienced network administrators who configure and maintain Cisco Nexus devices.

This guide is for network and server administrators with the following experience and knowledge:

- An understanding of virtualization
- Using VMware software to create a virtual machine and configure a VMware vSwitch

Note Knowledge of VMware vNetwork Distributed Switch is not required.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.

Convention	Description
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation for Nexus 1000V Series NX-OS Software for VMware vSphere

This section lists the documents used with the Cisco Nexus 1000V and available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V Documentation Roadmap

Cisco Nexus 1000V Release Notes

Cisco Nexus 1000V and VMware Compatibility Information

Install and Upgrade

Cisco Nexus 1000V Installation and Upgrade Guide

Configuration Guides

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V Interface Configuration Guide

Cisco Nexus 1000V Layer 2 Switching Configuration Guide

Cisco Nexus 1000V License Configuration Guide

Cisco Nexus 1000V Network Segmentation Manager Configuration Guide

Cisco Nexus 1000V Port Profile Configuration Guide

Cisco Nexus 1000V Quality of Service Configuration Guide

Cisco Nexus 1000V REST API Plug-In Configuration Guide

Cisco Nexus 1000V Security Configuration Guide

Cisco Nexus 1000V System Management Configuration Guide

Cisco Nexus 1000V vCenter Plugin Configuration Guide

Cisco Nexus 1000V VXLAN Configuration Guide

Programming Guide

Cisco Nexus 1000V XML API Configuration Guide

Reference Guides

Cisco Nexus 1000V Command Reference

Cisco Nexus 1000V Resource Availability Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide

Cisco Nexus 1000V Password Recovery Procedure

Cisco NX-OS System Messages Reference

Cloud Services Platform Documentation

The *Cisco Cloud Services Platform* documentation is available at http://www.cisco.com/en/US/products/ps12752/tsd_products_support_series_home.html.

Virtual Security Gateway Documentation

The *Cisco Virtual Security Gateway for Nexus 1000V Series Switch* documentation is available at http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html.

Virtual Wide Area Application Services (vWAAS) Documentation

The *Virtual Wide Area Application Services* documentation is available at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.

ASA 1000V Cloud Firewall Documentation

The *ASA 1000V Cloud Firewall* documentation is available at http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to one of the following:

- nexus1k-docfeedback@cisco.com

We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

CHAPTER 1

Overview

This chapter contains the following sections:

- Information About VXLANs, page 1
- Scalability, page 4
- Supported Features, page 5

Information About VXLANs

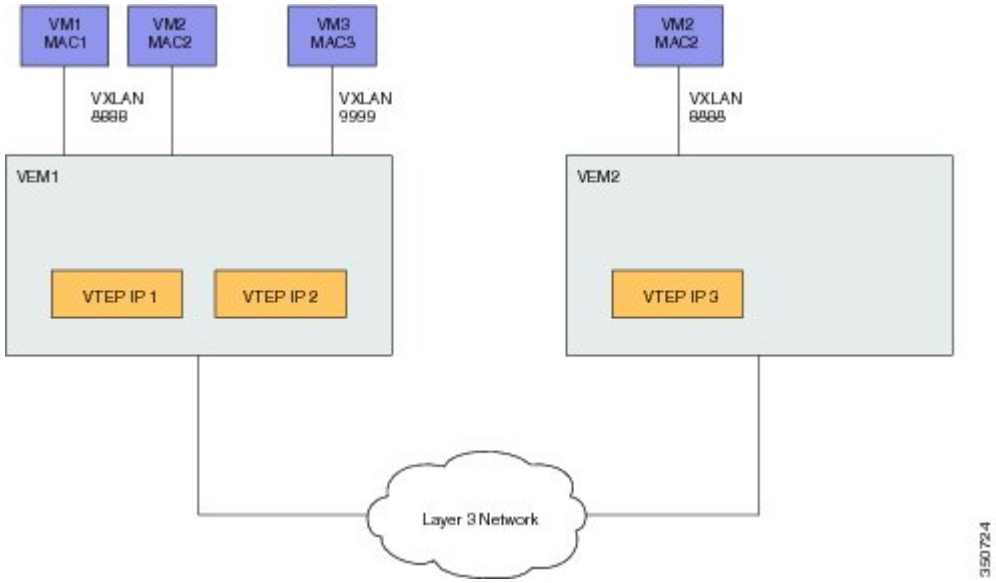
Overview of VXLANs

The Virtual Extensible LAN (VXLAN) technology enables you to create virtual domains by running a Layer 2 overlay network on top of Layer 3 with MAC-in-UDP encapsulation and a 24-bit VXLAN ID. The original Layer 2 frame from a Virtual Machine (VM) is encapsulated from within the Virtual Ethernet Module (VEM). Each VEM is assigned at least one IP address that is used as the source IP address when the encapsulated MAC frames are sent to other VEMs over the network.

The IP addresses, which are known as VXLAN Tunnel End Point (VTEP) IP addresses, are assigned to selected vmknics on the corresponding VEM. The encapsulation carries the VXLAN ID to scope the MAC

address of the payload frame. The VM's VXLAN ID is indicated within the port profile configuration of the vNIC and is applied when the VM connects to the network.

Figure 1: VXLAN Overview



A VXLAN supports two different modes for flood traffic:

- Multicast mode—A VXLAN uses an IP multicast network to send broadcast, multicast, and unknown unicast flood frames. Each multicast mode VXLAN has an assigned multicast group IP address. When a new VM joins a host in a multicast mode VXLAN, a VEM joins the assigned multicast group IP address by sending IGMP join messages. Flood traffic, broadcast, multicast and unknown unicast from the VM is encapsulated and is sent using the assigned multicast group IP address as the destination IP address. Packets sent to known unicast MAC addresses are encapsulated and sent directly to the destination server VTEP IP addresses.
- Unicast-only mode—A VXLAN uses each VEM's single unicast IP address as the destination IP address to send broadcast, multicast, and unknown unicast flood frames of the designated VTEP on each VEM that has at least one VM in the corresponding VXLAN. When a new VM joins the host in a unicast-mode VXLAN, a designated VTEP is selected for receiving flood traffic on that host. This designated VTEP is communicated to all other hosts through the Virtual Supervisor Module (VSM). Flood traffic (broadcast, multicast, and unknown unicast) is replicated on each VEM's designated VTEP in that VXLAN by encapsulating it with a VXLAN header. Packets are sent only to VEMs with a VM in that VXLAN. Packets that have a unicast MAC address are encapsulated and sent directly to the destination server's VTEP IP address.
    - MAC distribution mode (supported only in unicast mode)—In this mode, unknown unicast flooding in the network is eliminated. The VSM learns all the MAC addresses from the VEMs in all the VXLANs and distributes those MAC addresses with VTEP IP mappings to other VEMs. Therefore, there is no unknown unicast MAC address in the network when the VMs on the VEMs are communicating and controlled by the same VM.

Note MAC distribution works only for static MAC addresses. If dynamic MAC addresses are found on ports that use VXLANs that operate in MAC distribution mode, syslogs are generated to indicate that MAC distribution does not work with dynamic MAC addresses.

Note You can configure the above modes globally and override them for each bridge domain.

By default, if you upgrade the VSM from an earlier version of the Cisco Nexus 1000V to the current version with the segmentation feature enabled, all the VXLANs continue to operate in multicast mode. If you enable the feature when the VSM is running the current version of the Cisco Nexus 1000V, by default, the bridge domains change to unicast-only mode. You must explicitly enable MAC distribution mode because it is disabled by default.

After completing the software upgrade, you need to explicitly configure the segment mode to multicast mode.

Note During an upgrade, you cannot enable unicast-only mode unless you upgrade all VEMs and the VEM level.

VXLAN Tunnel Endpoints

Each VEM requires at least one IP/MAC address pair to terminate VXLAN packets. This IP/MAC address pair is known as the VXLAN Tunnel End Point (VTEP) IP/MAC addresses. The VEM supports IPv4 addressing for this purpose. The IP/MAC address that the VTEP uses is configured when you enter the **capability vxlan** command. You can have a maximum of four VTEPs in a single VEM.

One VTEP per VXLAN segment is designated to receive all broadcast, multicast, and unknown unicast flood traffic for the VEM.

When encapsulated traffic is destined to a VEM that is connected to a different subnet, the VEM does not use the VMware host routing table. Instead, the VTEPs initiate the Address Resolution Protocol (ARP) for remote VEM IP addresses. If the VTEPs in the different VEMs are in different subnets, you must configure the upstream router to respond by using the Proxy ARP.

VXLAN Gateway

VXLAN termination (encapsulation and decapsulation) is supported on virtual switches. As a result, the only endpoints that can connect into VXLANs are VMs that are connected to a virtual switch. Physical servers cannot be in VXLANs and routers or services that have traditional VLAN interfaces cannot be used by VXLAN networks. The only way that VXLANs can currently interconnect with traditional VLANs is through VM-based software routers.

The supported gateways are as follows:

- VMware vShield Edge

- Cisco VXLAN gateway
- Cisco ASA1000V

The configuration for such VLAN-VXLAN translation/mappings for the VXLAN gateway must be configured from the VSM and must always be a 1:1 mapping for each Layer 2 domain. Each VXLAN gateway can support multiple VLAN-VXLAN mappings.

VXLAN Trunks

A VXLAN trunk allows you to trunk multiple VXLANs on a single virtual Ethernet interface. In order to achieve this configuration, you must encapsulate a VLAN-VXLAN mapping on the virtual Ethernet interface.

VLAN-VXLAN mappings are applied on a virtual Ethernet interface using a port profile. A single port profile can support multiple VLAN-VXLAN mappings.

Multi-MAC Capability

You must use the multi-MAC capability feature to mark a virtual Ethernet interface as capable of sourcing packets from multiple MAC addresses. For example, you can use this feature if you have a virtual Ethernet port and you have enabled VXLAN trunking on it and the VM that is connected to the port bridges packets that are sourced from multiple MAC addresses.

By using this feature, you can easily identify such multi-MAC capable ports and handle live migration scenarios correctly for those ports.

Fragmentation

The VXLAN encapsulation overhead is 50 bytes. In order to prevent performance degradation due to fragmentation, the entire interconnection infrastructure between all VEMs that exchange VXLAN packets must be configured to carry 50 bytes more than what the VM VNICs are configured to send. For example, if the default VNIC configuration is 1500 bytes, the VEM uplink port profile, upstream physical switch port, and interswitch links, and any routers if present, must be configured to carry a maximum transmission unit (MTU) of at least 1550 bytes. If that is not possible, we recommend that you configure the MTU within the guest VMs to be smaller by 50 bytes.

If you do not configure a smaller MTU, the VEM attempts to notify the VM if it performs Path MTU (PMTU) Discovery. If the VM does not send packets with a smaller MTU, the VM fragments the IP packets. Fragmentation occurs only at the IP layer. If the VM sends a frame that is too large, the frame will be dropped after VXLAN encapsulation and if the frame does not contain an IP packet.

Scalability

Maximum Number of VXLANs

The Cisco Nexus 1000V supports up to 2048 VLANs and 2048 VXLANs with a combined maximum of 4096.

Supported Features

Jumbo Frames

Jumbo frames are supported by the Cisco Nexus 1000V if there is space on the frame to accommodate the VXLAN encapsulation overhead of at least 50 bytes, and the physical switch/router infrastructure has the capability to transport these jumbo-sized IP packets.

VXLAN Feature Disabled

As a safety precaution, do not use the **no feature segmentation** command if there are any ports associated with a VXLAN port profile. You must remove all associations before you can disable this feature. You can use the **no feature segmentation** command to remove all the VXLAN bridge domain configurations on the Cisco Nexus 1000V.

VXLAN Offload

The Cisco Nexus 1000V supports offloading VXLAN checksum and TSO computations of inner packets for VXLAN encapsulated packets. The VXLAN offload feature is supported only if an adapter supports the offload feature and VMware supports the offload feature on that adapter. To verify if the Cisco Nexus 1000V supports the VXLAN offload feature on an adapter, use the **vemcmd show pd-port** command on the host. The V flag in the Flags column indicates that the VXLAN offload feature is supported. The TSO computations are automatically offloaded when the VXLAN offload feature is supported.

CHAPTER 2

Configuring VXLANs

This chapter contains the following sections:

- Information About VXLANs, page 7
- Guidelines and Limitations for VXLANs, page 8
- Default Settings for VXLANs, page 9
- Configuring VXLANs, page 9
- Verifying the VXLAN Configuration, page 19
- Feature History for VXLAN, page 20

Information About VXLANs

Prerequisites for VXLANs

VXLANs have the following prerequisites:

- The Cisco Nexus 1000V uplink port profiles and all interconnecting switches and routers between the ESX hosts must have their supported maximum transmission unit (MTU) set to at least 50 bytes larger than the MTU of the Virtual Machines (VMs). For example, the VMs default to using a 1500 byte MTU (same as the uplinks and physical devices), so you must set them to at least 1550 bytes. If this configuration is not possible, you should lower all VM vNICs MTU to 50 bytes smaller than what the physical network supports, such as 1450 bytes. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide*.
- If the Cisco Nexus 1000V is using a port channel for its uplinks, you should set the load distribution algorithm to a 5-tuple hash (IP/Layer 4/Layer 4 ports). Use the same setting for any port channels on the physical switches. For more information, see the *Cisco Nexus 1000V Interface Configuration Guide*.
- VXLAN uses MAC in IP (UDP) with a destination port of 8472. You must allow this port through any intermediate firewall.
- If you are using the VXLAN multicast mode, you must configure an IGMP querier in the VXLAN transport VLANs.

Guidelines and Limitations for VXLANs

VXLAN has the following configuration guidelines and limitations:

- VXLANs in unicast-only mode are supported only between VEMs that are managed by a single VSM. A VXLAN in unicast-only mode cannot be shared across two different distributed virtual switches.
- When a VXLAN is configured in the unicast-only mode with MAC distribution enabled, the VXLAN gateway does not register any MAC addresses that it learns on the VLAN side. If these MAC addresses have not been learned yet, the traffic to these MAC addresses is delivered by replicating of unknown unicast packets to the VXLAN gateway. This is the only scenario where unknown unicast packets are replicated in the MAC distribution mode.
- Microsoft Network Load Balancing (NLB) servers in unicast mode require unknown unicast packets to be delivered to all the server ports, because the shared MAC address of the NLB servers is never discovered. This solution will break the unknown unicast semantics of unicast-only mode with MAC distribution. We recommend that you use either multicast mode or unicast-only mode without MAC distribution.
- You cannot enable the MAC distribution mode and the multi-MAC capability feature together. You must use either the MAC distribution or the muti-MAC capability feature.
- The Cisco Nexus 1000V switch in ESXi 5.5 supports VXLAN offload NICs. The Cisco Nexus 1000V switch is designed to assume that either all or none of the physical NICs (PNICs) in a port channel support the VXLAN offload capability.

VXLAN has the following configuration guidelines and limitations for changing the VXLAN configuration:

- Use the **segment mode unicast-only** command to change the global configuration mode from multicast to unicast. This command affects all bridge domains with no overrides.
- You can use multicast or unicast mode if you override the global configuration for the bridge domain by entering the **segment mode unicast-only** or **no segment mode unicast-only** commands.
- You can enable the segment distribution MAC command only after entering the **segment mode unicast-only** command.
- You can disable the segment distribution MAC address configuration globally by entering the **no segment distribution mac** command.
- You cannot use the **no segment mode unicast-only** command if you already entered the **segment distribution MAC** command.
- You must configure a multicast IP address that is required for a VXLAN that is in the multicast mode.
- If you remove the multicast IP address while VXLAN is in the multicast mode, the ports that use that VXLAN go to the inactive state.

Note Ports become inactive if you change the mode from unicast to multicast if a multicast IP address is not configured or a segment ID is removed.

Default Settings for VXLANs

The following table lists the default settings for VXLAN parameters.

Table 1: Default VXLAN Parameters

Parameter	Default
Feature Segmentation	Disabled

Configuring VXLANs

Initial Enabling of VXLANs

To enable a VXLAN, you must perform the following two procedures when you first configure a VXLAN.

- Configuring vmknics for VXLAN Encapsulation, on page 10
- Enabling VXLANs, on page 9

Enabling VXLANs

Before You Begin

Enter the **show system vem feature level** command to confirm that the feature level is 4.2(1)SV1(5.1) or a later release. If the feature level is not 4.2(1)SV1(5.1) or a later release, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature segmentation**	Enables the VXLAN.
Step 3	switch(config)# **show feature** | **grep segmentation**	(Optional) Displays whether the VXLAN is enabled.
Step 4	switch (config)# [**no**] **segment-mode unicast-only**	Configures the global configuration mode for all VXLAN bridge domains. If the configuration mode is not entered, the global mode is unicast-only mode without MAC distribution.
Step 5	switch (config)# [**no**] **segment distribution mac**	Enables or disables MAC distribution globally. All bridge domains with default MAC distribution mode

	Command or Action	Purpose
		will inherit this configuration and enable or disable MAC distribution.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to enable the segmentation feature:

```
switch# configure terminal
switch(config)# feature segmentation
switch(config)# show feature | grep segmentation
network-segmentation 1 disabled
segmentation         1 enabled
switch(config)# copy running-config startup-config
```

Configuring vmknics for VXLAN Encapsulation

Before You Begin

- Identify a VLAN to be used for transporting VXLAN-encapsulated traffic.
- Ensure that it is configured on the uplink port profile for all VEMs on which the VXLAN can be configured.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile type veth** *profilename*	Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics: • *profilename*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V. **Note** If a port profile is configured as an Ethernet type, it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **vmware port-group** *name*	Designates the port profile as a VMware port group. The port profile is mapped to a VMware port group of the same name unless you specify a name here. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on vCenter Server.

	Command or Action	Purpose
Step 4	switch(config-port-prof)# **switchport mode access**	Designates the interfaces as switch access ports (the default).
Step 5	switch(config-port-prof)# **switchport access vlan** *id*	Assigns a VLAN ID to this port profile. **Note** A VLAN ID must be created and should be in the active state.
Step 6	switch(config-port-prof)# **capability vxlan**	Assigns the VXLAN capability to the port profile to ensure that the interfaces that inherit this port profile are used as sources for VXLAN-encapsulated traffic.
Step 7	switch(config-port-prof)# **no shutdown**	Administratively enables all ports in the profile.
Step 8	switch(config-port-prof)# **state enabled**	Sets the operational state of a port profile.
Step 9	switch(config-port-prof)# **show port-profile name** *profilename*	Displays the port profile configuration.
Step 10	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure a vmknic for VXLAN encapsulation:

```
switch# configure terminal
switch(config)# port-profile type veth vmknic-pp
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access vlan 100
switch(config-port-prof)# capability vxlan
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# show port-profile name vmknic-pp
port-profile vmknic-pp
type: Vethernet
description:
status: enabled
max-ports: 32
min-ports: 1
inherit:
config attributes:
switchport mode access
switchport access vlan 100
capability vxlan
no shutdown
evaluated config attributes:
switchport mode access
switchport access vlan 100
capability vxlan
no shutdown
assigned interfaces:
port-group: vmknic-pp
system vlans: none
capability l3control: no
capability iscsi-multipath: no
capability vxlan: yes
```

```
capability l3-vservice: no
port-profile role: none
port-binding: static

switch(config-port-prof)#
switch(config-port-prof)# copy running-config startup-config
```

What to Do Next

The vSphere administrator must create a new vmknic on each ESX/ESXi host and assign the previously created port profile to this vmknic. IP address and netmask should be assigned to the vmknic. This IP address will be used for VXLAN packet encapsulation. Use the **show module vteps** to view the interfaces on the VSM.

Creating a Bridge Domain

You are limited to creating a maximum of 2048 VXLAN bridge domains.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **bridge-domain** *name-string*	Creates a VXLAN and associates an identifying name to it.
Step 3	switch(config-bd)# **segment id** [*number*]	Specifies the VXLAN segment ID. Only one bridge domain can use a particular segment ID value. Valid values are from 4096 to 16000000. (1 to 4095 are reserved for VLANs.)
Step 4	switch(config-bd)# **group** *ipaddr*	(Optional) Associates the multicast group for broadcasts and floods. **Note** Reserved multicast addresses are not allowed.
Step 5	switch(config-bd)# **show bridge-domain** *name-string*	(Optional) Displays bridge domain information.
Step 6	switch(config-bd)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to create a VXLAN:

```
switch# configure terminal
switch(config)# bridge-domain tenant-red
switch(config-bd)# segment id 4096
switch(config-bd)# group 239.1.1.1
switch(config-bd)# show bridge-domain tenant-red
Bridge-domain tenant-red (0 ports in all)
Segment ID: NULL
Mode: Unicast-only (default)
```

```
MAC Distribution: Disable (default)
Group IP: 239.1.1.1
State: UP Mac learning: Enabled
switch(config-bd)#
switch(config-bd)# copy running-config startup-config
```

Configuring the Bridge Domain Mode

You can configure a bridge domain in the bridge-domain mode or global mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch# **bridge-domain***bd-name*	Creates a bridge domain.
Step 3	switch (config-bd)# [**no**] **segment mode unicast-only** | **default segment mode**	Configures the segment mode as unicast only. The mode can be configured globally or for a specific bridge domain. When configured under a specific bridge domain, the mode is treated as an override to the global configuration for that specific bridge domain. Any change in the global configuration affects all the bridge domains that do not have overrides. The mode configuration on a specific bridge domain overwrites the global bridge domain. The overrides configured on the bridge domain can be removed by using the **default segment mode**. **Note** Use the **no segment mode unicast-only** command to override the configuration under a bridge domain. If you have unicast enabled globally, the bridge domain can use the multicast mode. To override, use the **default segment mode** command. **Note** This command cannot be performed globally or under a bridge domain if the **segment distribution MAC** feature is configured.
Step 4	switch (config-bd)# [no] **segment distribution mac** | **default segment distribution mac**	Enables MAC distribution for the bridge domain. **Note** To configure an override under a bridge domain, you must enter the **segment mode unicast-only** command as an override first.

This example shows how to configure a bridge domain:

Note The ports are inactive if a segment ID is not configured for a bridge domain and if a multicast IP address is not configured when global configuration or a bridge domain override has the **no segment mode unicast-only** configuration.

```
config terminal
bridge-domain domain-660
```

```
segment mode unicast-only
segment distribution mac
```

Creating a Port Profile Configured to Use a VXLAN

Alternatively, you can associate ports with a bridge domain by modifying the configuration of an existing virtual Ethernet port profile to use VXLANs instead of VLANs. To do so, enter the **switchport access bridge-domain name** command on a profile with switchport mode access configured.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**vethernet**}] *name*	Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics: • name—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V. • type—The port profile type is virtual Ethernet. Once configured, the type cannot be changed. The default is the virtual Ethernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **vmware port-group** [*pg_name*]	Designates the port profile as a VMware port group. The port profile is mapped to a VMware port group of the same name unless you specify a name here. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on vCenter Server.
Step 4	switch(config-port-prof)# **switchport mode access**	Designates that the interfaces are to be used as trunking ports. A trunk port transmits untagged packets for the native VLAN and transmits encapsulated, tagged packets for all other VLANs.
Step 5	switch(config-port-prof)# **switchport access bridge-domain** <*bridge-domain name*>	Assigns a VXLAN bridge domain to this port profile. You must configure the bridge domain with its segment ID for the port to be active. You should configure a multicast IP address if you prefer multicast mode. The multicast mode is

	Command or Action	Purpose
		displayed in the running configuration as **no segment mode unicast-only**.
Step 6	switch(config-port-prof)# **no shutdown**	Administratively enables all ports in the profile.
Step 7	switch(config-port-prof)# **state enabled**	Sets the operational state of a port profile.
Step 8	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	(Optional) Displays the configuration for verification.
Step 9	switch(config-port-prof)# **show running-config bridge-domain**	(Optional) Displays the segmentation configuration.
Step 10	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to create a port profile configured to use a VXLAN:

```
switch# configure terminal
switch(config)# port-profile tenant-profile
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access bridge-domain tenant-red
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# show port-profile name tenant-profile
port-profile tenant-profile
type: Vethernet
description:
status: enabled
max-ports: 32
min-ports: 1
inherit:
config attributes:
switchport mode access
switchport access bridge-domain tenant-red
no shutdown
evaluated config attributes:
switchport mode access
switchport access bridge-domain tenant-red
no shutdown
assigned interfaces:
port-group: tenant-profile
system vlans: none
capability l3control: no
capability iscsi-multipath: no
capability vxlan: no
capability l3-vservice: no
port-profile role: none
port-binding: static

switch(config-port-prof)#
switch(config-port-prof)# show running-config bridge-domain
switch(config-port-prof)# copy running-config startup-config
```

Removing Ports from a VXLAN

By performing this procedure, you move the ports to the default VLAN.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**vethernet**}] *name*	Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics: • **name—**The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V. • **type—**The port profile type is vEthernet. Once configured, the type cannot be changed. The default is the vEthernet type. Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs). **Note** If a port profile is configured as an Ethernet type, it cannot be used to configure VMware virtual ports.
Step 3	switch(config-port-prof)# **no switchport access bridge-domain**	Removes the VXLAN bridge domain from this port profile.
Step 4	switch(config-port-prof)# **show port-profile usage**	(Optional) Displays a list of interfaces that inherited a port profile.
Step 5	switch(config-port-prof)# **show bridge-domain**	(Optional) Displays all bridge domains.
Step 6	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to remove ports from a VXLAN:

```
switch# configure terminal
switch(config)# port-profile tenant-profile
switch(config-port-prof)# no switchport access bridge-domain tenant-red
switch(config-port-prof)# show port-profile usage
switch(config-port-prof)# show bridge-domain
switch(config-port-prof)# copy running-config startup-config
```

Deleting a VXLAN

When you delete an existing bridge domain with ports on it, all the ports are moved to a down state and traffic stops flowing.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no bridge-domain group-red**	Deletes a VXLAN.
Step 3	switch(config-bd)# **show bridge-domain**	(Optional) Displays all bridge domains.
Step 4	switch(config-bd)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

This example shows how to delete a VXLAN:

```
switch# configure terminal
switch(config)# no bridge-domain group-red
switch(config)# show bridge-domain
switch(config)# copy running-config startup-config
```

Disabling Segmentation

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **show bridge-domain**	Displays all bridge domains. **Note** You must identify all bridge domains with nonzero port counts.
Step 3	switch(config)# **show running port-profile**	(Optional) Displays the running configuration for all port profiles. **Note** You must use this command to identify which port profiles have bridge domains identified in Step 2 configured.
Step 4	switch(config)# **port-profile** *name*	Names the port profile and enters port profile configuration mode. If the port profile does not already exist, it is created using the following characteristics:

	Command or Action	Purpose
		name—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V. **Note** If a port profile is configured as an Ethernet type, it cannot be used to configure VMware virtual ports.
Step 5	switch(config-port-prof)# **no switchport access bridge-domain** *name-string*	Removes the VXLAN bridge domain from this port profile and moves the ports to VLAN1.
Step 6	switch(config-port-prof)# **show port-profile usage**	(Optional) Displays a list of interfaces that inherited a port profile.
Step 7	switch(config-port-prof)# **show bridge-domain**	(Optional) Displays all bridge domains.
Step 8	switch(config-port-prof)# **no feature segmentation**	Removes the segmentation feature.
Step 9	switch(config-port-prof)# **show feature | grep segmentation**	(Optional) Displays if the segmentation feature is running or not running.
Step 10	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to disable segmentation:

```
switch# configure terminal
switch(config)# show bridge-domain

Global Configuration:
Mode: Unicast-only
MAC Distribution: Disable

Bridge-domain tenant-red (4 ports in all)
Segment ID: 4096 (Manual/Active)
Mode: Unicast-only
MAC Distribution: Disable
Group IP: NULL
State: UP Mac learning: Enabled
Veth1, Veth2, Veth4, Veth11

switch(config)# show running-config port-profile
port-profile default max-ports 32
port-profile default port-binding static
port-profile type ethernet Unused_Or_Quarantine_Uplink
vmware port-group
shutdown
description Port-group created for Nexus1000V internal usage. Do not use.
state enabled
port-profile type vethernet Unused_Or_Quarantine_Veth
vmware port-group
shutdown
description Port-group created for Nexus1000V internal usage. Do not use.
```

```
state enabled
port-profile type vethernet tenant-profile
vmware port-group
switchport mode access
switchport access bridge-domain tenant-red
no shutdown
state enabled

switch(config)#
switch(config-port-prof)# show port-profile usage

port-profile Unused_Or_Quarantine_Uplink

port-profile Unused_Or_Quarantine_Veth

port-profile tenant-profile
Vethernet1
Vethernet2
Vethernet4
Vethernet11

switch(config-port-prof)# show bridge-domain

Global Configuration:
Mode: Unicast-only
MAC Distribution: Disable

Bridge-domain tenant-red (0 ports in all)
Segment ID: 4096 (Manual/Active)
Mode: Unicast-only
MAC Distribution: Disable
Group IP: NULL
State: UP Mac learning: Enabled

switch(config-port-prof)#
switch(config-port-prof)# no feature segmentation
switch(config-port-prof)# 2013 May 23 05:34:42 switch-cy %SEG_BD-2-SEG_BD_DISABLED: Feature
 Segmentation disabled

switch(config-port-prof)# show feature | grep seg_bd
- NR - 1 - seg_bd
```

Verifying the VXLAN Configuration

To display the VXLAN configuration information, perform one of the following tasks:

Command	Purpose
show feature | grep segmentation	Displays if the segmentation feature is running.
show bridge-domain	Displays all bridge domains with the mode.
show bridge-domain vteps	Displays the bridge domain-to-VTEP mappings that are maintained by the VSM and are pushed to all VEMs.
show bridge-domain mac *bd-name*	Displays all the MAC addresses that are learned by the VSMs on VXLANs that are configured with the MAC distribution feature.
show run bridge-domain	Displays the running bridge domain.

Command	Purpose
show bridge-domain *bd-name*	Displays the specified bridge domain.
show bridge-domain *bd-name* **vteps**	Displays the specific bridge domain-to-VTEP mappings that are maintained by the VSM and are pushed to all VEMs.
show interface brief	Displays a short version of the interface configuration.
show interface switchport	Displays information about switchport interfaces.
show module vteps	Displays the IP addresses available on each module that can be used for VXLAN Tunnel Endpoints.

Feature History for VXLAN

Feature Name	Releases	Feature Information
Enhanced VXLAN	4.2(1)SV2(2.1)	Added the enhanced VXLAN commands.
VXLAN	4.2(1)SV1(5.1)	Introduced the Virtual Extensible Local Area Network (VXLAN) feature.

CHAPTER 3

Installing and Configuring VXLAN Gateway

This chapter contains the following sections:

- Information About the VXLAN Gateway Deployment, page 21
- Guidelines and Limitations, page 22
- Configuring VSMs, page 23
- Configuring VXLAN Termination/VTEP on the VXLAN Gateway, page 25
- Installing a VXLAN Gateway as a Virtual Service Blade, page 27
- Configuring High Availability, page 31
- Verifying the VXLAN Gateway Installation and Configuration, page 32
- Managing the VXLAN to VLAN Mappings on the VXLAN Gateway, page 38
- Deleting the VXLAN Gateway, page 39
- Feature History for VXLAN Gateways, page 40

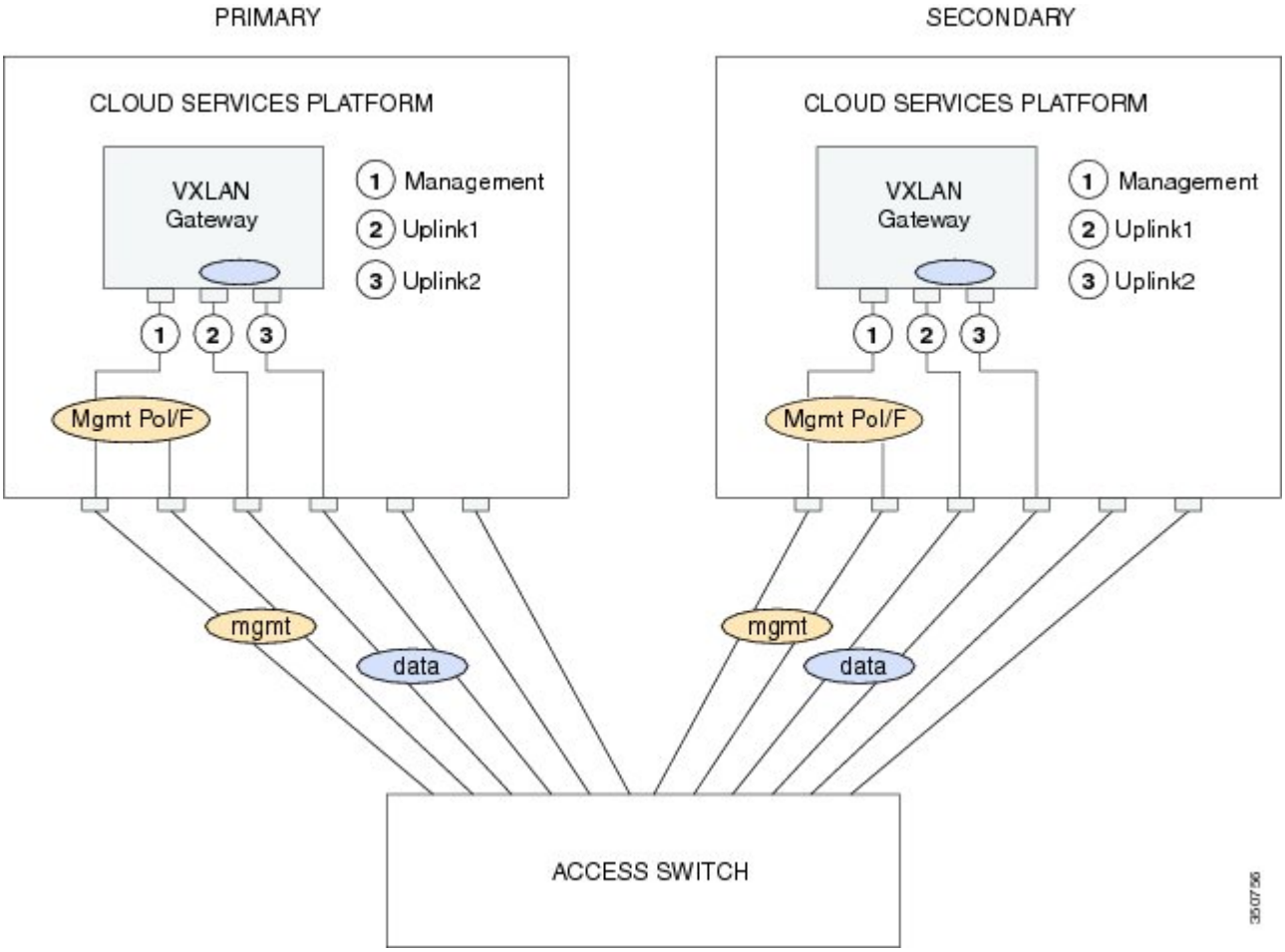
Information About the VXLAN Gateway Deployment

The VXLAN gateway has the following deployment requirements:

- The VXLAN gateway is deployed only on the Cisco Cloud Services platform Release 4.2(1)SP1(6.1) or later releases.
- You must connect the Cloud Services Platform appliance to a switch that supports Link Aggregation Control Protocol (LACP) based or statically configured port channels and VLAN-based trunk interfaces.
- Ensure that you install or upgrade the Virtual Supervisor Module (VSM) to the current release of Cisco Nexus 1000V software. When you upgrade from an older version of the VSM, use the **show system vem feature level** command to check if you have the current version of the Cisco Nexus 1000V software.
- You must have an advanced mode license to set up the VSM .
- vCPU or Memory requirements—You will need three vCPUs, 2-GB RAM, and 3-GB virtual disk space for each VXLAN gateway Virtual Service Blade (VSB).

This figure shows the VXLAN gateway deployment.

Figure 2: VXLAN Gateway Deployment



Guidelines and Limitations

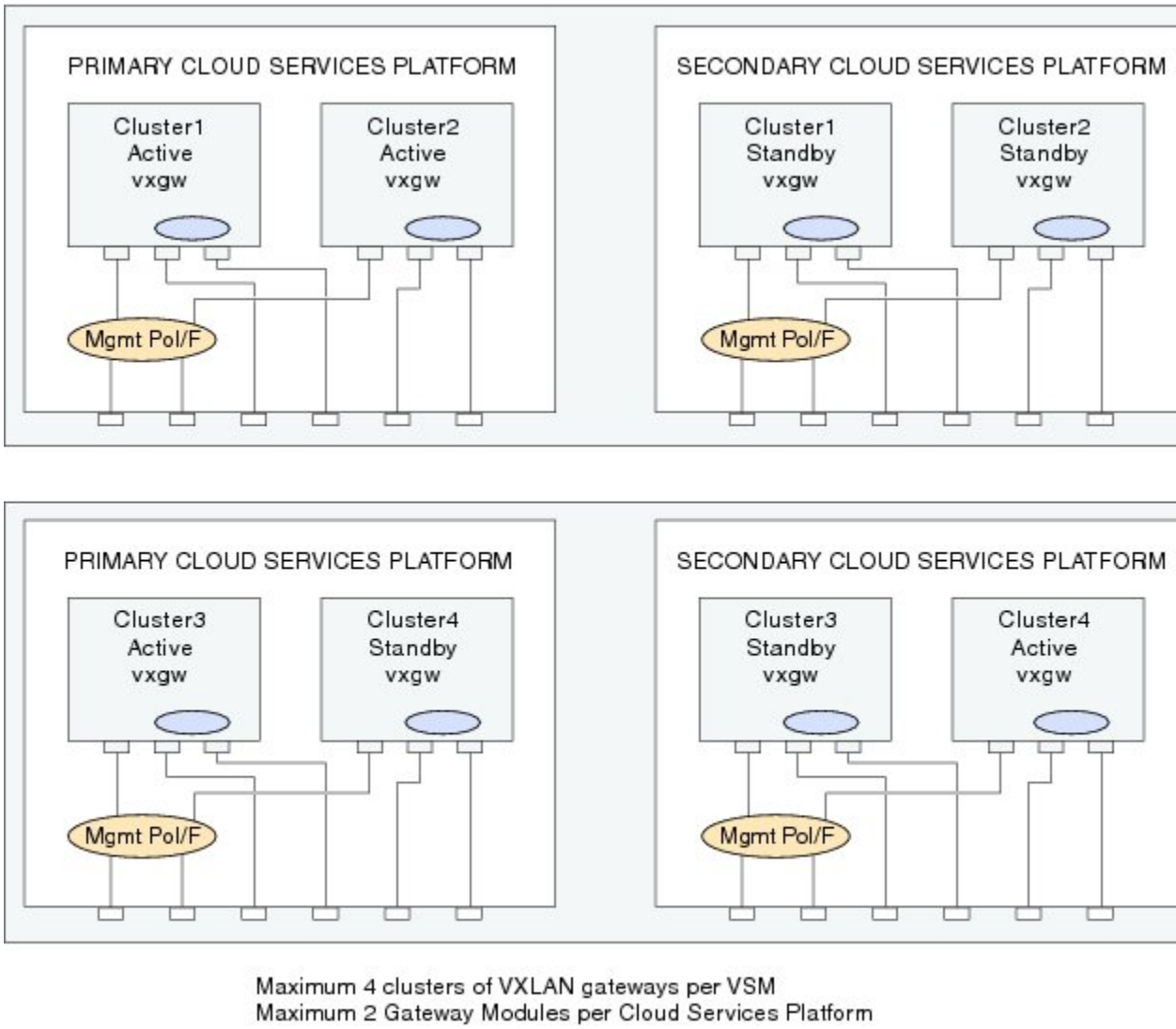
VXLAN gateways have the following configuration guidelines and limitations:

- You must configure the VSM to use the Layer 3 control. We strongly recommend that the VSM Layer 3 control is through mgmt 0. For more information about Layer 3 control, see the *Cisco Nexus 1000V Installation and Upgrade Guide* and *Cisco Nexus 1000V System Management Configuration Guide*.
- You must configure the uplink for the gateway module as a LACP or a static port channel. The VXLAN gateway does not function if gateways are configured in the MAC-pinning mode.
- A single VSM can manage a maximum of four VXLAN gateway high availability (HA) clusters.
- You must configure the underlying Cloud Services Platform with an uplink type that is flexible (type 5). VXLAN gateways use two physical interfaces. You must set the interfaces in the passthrough mode. In addition, you must set at least one physical or a port channel interface must be set up to carry management traffic.

- Ensure you do not configure PVLAN on the VLANs used for VXLAN-VLAN mappings.

The following illustration displays the maximum allowed VXLAN gateway deployment managed by a single VSM. It displays four Cloud Services Platform devices and each Cloud Services Platform device hosting two VXLAN gateway modules. Four HA clusters of gateway modules are setup with each cluster consisting of an active/standby pair of modules.

Figure 3: VXLAN Gateway HA Pairs



Configuring VSMs

Before installing the VXLAN gateway module on the Cloud Services Platform, you must create two port profiles on the VSM, one for the uplinks on the gateway and one for the VTEP interface.

Note You can configure the VXLAN gateway across multiple devices. This chapter explains the commands that you can execute on different devices using the following the prompts:

- VSM— Virtual Supervisor Module
- CSP— Cloud Services Platform
- GW— VXLAN gateway VSB

To create a suitable port-profile that can be applied to the uplink of a VXLAN gateway service module, use the procedure below:

Before You Begin

- Ensure that the VSM is configured in the Advanced mode by entering the **svs switch edition advanced** configuration command to enable Advanced mode.
- Ensure LACP is configured by entering the **feature lacp** configuration command on the VSM.
- Offload the LACP operation by entering the **lacp offload** configuration command on the VSM..
- Ensure that the VXLAN feature is enabled on the VSM by entering the **feature segmentation** configuration command to enable VXLANs on the VSM.
- Ensure that the VXLAN gateway is enabled on the VSM by entering the **feature vxlan-gateway** configuration command.
- Ensure that the interfaces of the upstream switch are configured with matching port channel and VLAN trunk configuration.

Procedure

	Command or Action	Purpose
Step 1	vsm# **configure terminal**	Enters global configuration mode.
Step 2	vsm(config)# **port profile type ethernet** *<name>*	Creates a port profile of type ethernet for the VXLAN gateway uplink. **Note** You must provide a port-profile name when prompted while executing the setup script described under Setup Script to Configure the VXLAN Gateway..
Step 3	vsm(config-port-prof)# **switchport mode trunk**	Designates that the interfaces are to be used as trunking ports. A trunk port transmits untagged packets for the native VLAN and transmits encapsulated, tagged packets for all other VLANs.
Step 4	vsm(config-port-prof)# **switchport trunk allowed vlan** *<vlan list>*	Specifies the list of VLANs allowed on the gateways uplink. This list should consist of all the mapped VLANs and the VLAN for the VTEP virtual interface.
Step 5	vsm(config-port-prof)# **mtu** *<mtu size in bytes>*	Designates the MTU size. For VXLAN traffic to be functional, you must set the MTU size as 1550. If you do not set the MTU

	Command or Action	Purpose
		size, the default of 1500 is used. The size must be an even number between 1500 and 9000. The MTU configured on an interface takes precedence over the MTU configured on a port profile.
Step 6	vsm(config-port-prof)# **service instance** *<1-4096>*	(Optional) Defines a place holder for mappings. The range is from 1 to 4096. **Note** You do not need to execute the service instance and the encapsulation command at this stage to bring up the gateway. They are optional and you can add the mappings later once the port-profiles are configured.
Step 7	vsm(config-port-prof-srv)# **encapsulation dot1q** *<vlan id>* **bridge-domain** *<bd-name>*	(Optional) Maps a VLAN to a VXLAN. The VXLAN is specified through the bridge-domain name. The bridge-domain name and VLAN-ID you provide are not created during the port-profile configuration. The bridge-domain name and the VLAN ID you provide should be in an active state or the mapping is held in pending state until you create the bridge-domain name and VLAN ID.
Step 8	vsm(config-port-prof-srv)# **exit**	(Optional) Exits from the service instance mode.
Step 9	vsm(config-port-prof)# **channel-group auto mode active**	Configures port channel mode as LACP.
Step 10	vsm(config-port-prof)# **no shutdown**	Administratively enables all ports in the profile.
Step 11	vsm(config-port-prof)# **state enabled**	Enables the port profile and applies its configuration to the assigned ports.

This example displays how to configure and display the gateway mappings:

```
vsm(config)# port-profile type ethernet gw-uplink
vsm(config)# switchport mode trunk
vsm(config)# switchport trunk allowed vlan 1545
vsm(config)# mtu 1550
vsm(config-port-prof)# service instance 1
vsm(config-port-prof-srv)# encapsulation dot1q 753 bridge-domain bd-753
vsm(config-port-prof-srv)# exit
vsm(config-port-prof)# channel-group auto mode active
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
```

Configuring VXLAN Termination/VTEP on the VXLAN Gateway

To create a suitable port-profile that can be applied to the VTEP virtual interface, use the procedure below:

Procedure

	Command or Action	Purpose
Step 1	vsm# **configure terminal**	Enters global configuration mode.
Step 2	vsm(config) # **port-profile type vethernet** *<port-profile name>*	Configures a port profile for the VTEP on the VXLAN gateway. **Note** You must provide a port-profile name when prompted while executing the setup script described under Setup Script to Configure the VXLAN Gateway..
Step 3	vsm(config-port-prof) # **switchport mode access**	Designates that the interfaces are to be used as a trunking ports. A trunk port transmits untagged packets for the native VLAN and transmits encapsulated, tagged packets for all other VLANs.
Step 4	vsm(config-port-prof) # **switchport access vlan** *<vlan-id-access>*	Assigns an access VLAN ID to this port profile. The VLAN ID provided must be added to the allowed VLAN set of the uplink port profile. This VLAN should not be mapped to any VXLAN. **Note** If you do not specify a VLAN ID, VLAN 1 is used automatically.
Step 5	vsm(config-port-prof) # **capability vxlan**	Configures the capability VXLAN feature on the specified virtual ethernet port and enables encapsulation and decapsulation of VXLAN packets.
Step 6	vsm(config-port-prof) # **transport ip address** *<IP address> <network mask>* **gateway** *< IP address>*	Configures VXLAN termination or a VTEP on the VXLAN gateway. Creating VTEP port-profile is similar to the steps described under Configuring vmknics for VXLAN Encapsulation except the **vmware port-group** command which is not supported on the VXLAN Gateway.
Step 7	vsm(config-port-prof)# **no shutdown**	Administratively enables all ports in the profile.
Step 8	vsm(config-port-prof)# **state enabled**	Enables the port profile and applies its configuration to the assigned ports.

This example displays how to configure VXLAN termination or VTEP on the VXLAN gateway:

```
vsm# configure terminal
vsm(config)# port-profile type vethernet gw-vtep
vsm(config-port-prof)# switchport mode access
vsm(config-port-prof)# switchport access vlan 760
vsm(config-port-prof)# capability vxlan
vsm(config-port-prof)# transport ip address 192.168.1.253 255.255.255.0 gateway 192.168.1.1
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
```

Installing a VXLAN Gateway as a Virtual Service Blade

You can install a VXLAN Gateway as a VSB on all Cisco Cloud Services Platforms. To do this, log into the Cloud Services Platform and follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	CSP# **copy scp:**// *<server where the VXGW image is located> < source path > < iso image of vxlan gw > < bootflash:repository >*	Copies the VXLAN gateway image to bootflash/repository on the CCPA Manager.
Step 2	CSP# **configure terminal**	Enters global configuration mode.
Step 3	CSP(config) # **virtual-service-blade** *<name of the VXLAN GW VSB>*	Creates a VXLAN gateway VSB.
Step 4	CSP(config-vsb-config) # **virtual-service-blade-type new** *<iso image of the vxlan gw>*	Deploys the downloaded VXLAN gateway. The image is always populated from the bootflash or repository and there is no need to specify the path.
Step 5	CSP(config-vsb-config) # **interface gw-uplink1 uplink** *<Physical-Interface Cloud Services Platform>*	Assigns a physical interface on the Cloud Services Platform to the gateway-uplink. GigabitEthernet3 through GigabitEthernet6 are available in the flexible mode physical interfaces. You must configure the port channels using LACP on the upstream switches.
Step 6	CSP(config-vsb-config) # **interface gw-uplink1 mode passthrough**	Configures the gateway uplink as passthrough. The corresponding GigabitEthernet interface cannot be shared with other VSBs on the Cloud Services Platform.
Step 7	CSP(config-vsb-config) # **interface gw-uplink2 uplink** *<Physical-Interface Cloud Services Platform>*	Assigns a physical interface on the Cloud Services Platform to the gateway-uplink. GigabitEthernet3 through GigabitEthernet6 are available in the flexible mode physical interfaces. You must configure the port channels using LACP on the upstream switches.
Step 8	CSP(config-vsb-config) # **interface gw-uplink2 mode passthrough**	Configures the gateway uplink as passthrough. The corresponding GigabitEthernet interface cannot be shared with other VSBs on the Cloud Services Platform.
Step 9	CSP(config-vsb-config) # **interface management vlan** *<vlan id>*	Allows the specified VLAN ID on the management uplink. The VLAN range is from 1 to 4096.
Step 10	CSP(config-vsb-config) # **interface management uplink** *<interface>*	The interface can either be a physical interface of the Cloud Services Platform or a port channel interface previously created on the Cloud Services Platform.

	Command or Action	Purpose
Step 11	Use one of the following commands to deploy a gateway: • CSP(config-vsb-config) # **enable** • CSP(config-vsb-config) # **enable primary** • CSP(config-vsb-config) # **enable secondary**	Use the **enable** command to install two VSBs, one on the primary Cloud Services Platform and another on the secondary cloud services platform. Use the **enable primary** command to deploy the gateway in standalone mode on the primary Cloud Services Platform. Use the **enable secondary** command to deploy the gateway in standalone mode on the secondary Cloud Services Platform. Initiates a setup script to configure the VXLAN gateway, IP address, subnet mask, gateway, hostname, and password for the VXLAN gateway VSB. You are also required to specify the details of the VSMs domain ID, IP address, primary and secondary MAC addresses on the control interface. For more information, see Setup Script to Configure the VXLAN Gateway.

This example shows how to bring up a gateway as a VSB on a VSA pair:

```
CSP(config)# virtual-service-blade VXLAN-GW
CSP(config-vsb-config)# virtual-service-blade-type new vxgw.4.2.1.SV2.2.0.264.iso
CSP(config-vsb-config)# interface gw-uplink1 uplink GigabitEthernet3
CSP(config-vsb-config)# interface gw-uplink2 uplink GigabitEthernet4
CSP(config-vsb-config)# interface gw-uplink1  mode passthrough
CSP(config-vsb-config)# interface gw-uplink2  mode passthrough
CSP(config-vsb-config)# interface management uplink GigabitEthernet1
CSP(config-vsb-config)# interface management vlan 751
CSP(config-vsb-config)# enable
```

Setup Script to Configure the VXLAN Gateway

After you enter enable while installing a VXLAN gateway as a VSB, the setup script to configure the VXLAN gateway is executed. This section describes the setup script to configure the following parameters on the VXLAN gateway:

- IP address, network mask, and default gateway for both the primary and secondary VXLAN Gateway Management interface
- VSM details—Domain ID, IP address, primary MAC address, and secondary MAC address of the VSM control interface
- Port profiles used for the VXLAN gateway uplink and VTEP

Procedure

Step 1 On the command prompt, enter the VSB image and press Enter.

```
Enter VSB image:x.x.x.x.x.x.x.iso: [vxgw.4.2.1.SV2.1.0.246.iso]
```

Step 2 Enter the VSM domain ID. The range is from 1 to 4095.

```
Enter domain [1-4095]:405
```

Note You can get the domain ID by entering the **show svs domain** command on the VSM.

Step 3 Enter the management IP version.

```
Management IP version [V4]:v4
```

Step 4 Configure the management IP address to interface mgmt 0 on the VXLAN gateway deployed on the Primary Cloud Services Platform.

```
Enter management IP address of service module on primary: 192.168.1.104
```

Note If you are deploying the gateway in the standalone mode on the secondary Cloud Services Platform, enter the IP address, network mask, and the default gateway address for the primary as 0.0.0.0.

Step 5 Enter the management subnet mask.

```
Enter management subnet mask of service module on primary: 255.255.255.0
```

Step 6 Enter the management default gateway.

```
Enter default gateway IP address of service module on primary: 192.168.1.1
```

Step 7 Configure the management IP address to interface mgmt 0 on the VXLAN gateway deployed on the secondary Cloud Services Platform.

```
Enter management IP address of service module on secondary: 192.168.1.105
```

Note If you are deploying the gateway in the standalone mode on the primary Cloud Services Platform, enter the IP address, network mask, and the default gateway address for the secondary as 0.0.0.0.

Note In a HA deployment, we recommend that the IP address you provide is in the same subnet as the one provided in Step 5.

Step 8 Enter the management subnet mask.

```
Enter management subnet mask of service module on secondary: 255.255.255.0
```

Step 9 Enter the management interface default gateway.

```
Enter default gateway IP address of service module on secondary: 192.168.1.1
```

Step 10 Enter the VXLAN Gateway hostname.

```
Enter hostname: VXLAN-GW-DOCS
```

Step 11 Enter the login credentials.

```
Enter the password for admin:Sfish123
```

Step 12 Enter the IP address of the VSM.

```
VSM L3 Ctrl IPv4 address:192.168.1.210
```

Step 13 Configure the MAC address of the control interface on the primary VSM.

```
VSM Primary MAC address: 0050.56b5.07d0
```

Note You can get the MAC address using the **show interface control 0** command on the primary VSM.

Step 14 Enter the MAC address of the secondary VSM.

```
VSM Standby MAC address: 0050.56b5.07d3
```

Note You can get the MAC address by entering the **show vms internal info** command on the secondary VSM.

Step 15 Enter the uplink trunk port profile configured on the VSM.

```
Enter VSM uplink port-profile name: gw-uplink
```

Note Enter the dedicated uplink trunk port-profile for the VXLAN gateway pair created on the VSM.

Step 16 Enter the VTEP profile name.

```
Enter VTEP port-profile name: gw-vtep
```

Note Enter the same VTEP port-profile name created on the VSM.

This example shows how to bring up the VXLAN gateway:

```
CSP(config-vsb-config)# enable
Enter vsb image: [vxgw.4.2.1.SV2.2.0.264.iso]
Enter the VSM domain id[1-4095]: 405
Enter Management IP version [V4]: [V4]
Enter Management IP address of service module on primary: 192.168.1.104
Enter Management subnet mask of service module on primary: 255.255.255.0
Enter default gateway IP address of service module on primary: 192.168.1.1
Enter management IP address of service module on secondary: 192.168.1.105
Enter management subnet mask of service module on secondary: 255.255.255.0
Enter default gateway IP address of service module on secondary: 192.168.1.1
Enter HostName: VXLAN-GW-DOCS
Enter the password for 'admin': Sfish123
VSM L3 Ctrl IPv4 address : 192.168.1.210
VSM Primary MAC Address: 0050.56b5.07d0
VSM Standby MAC Address: 0050.56b5.07d3
Enter VSM uplink port-profile name: gw-uplink
Enter VTEP port-profile name: gw-vtep
Note: VSB installation is in progress, please use show virtual-service-blade commands to
check the installation status.
CSP(config-vsb-config)#
```

Modifying the Initial Setup Script Parameters

After executing the setup script for the first time, if you need to modify any of the setup parameters, use the following commands on the VSM:

Note If an HA pair is installed, ensure that you apply the same changes individually on both the gateway modules.

Note Ensure the port profile that you update is first saved on the VSM.

Procedure

	Command or Action	Purpose
Step 1	vsm(config)# **service** <*module*> **update port-profile type ethernet name** <*VXLAN Gateway Uplink port-profile name*>	Modifies the VXLAN gateway uplink port-profile from the VSM.
Step 2	vsm(config)# **service** <*module*> **update port-profile type vethernet name** <*VXLAN Gateway VTEP port-profile name*>	Modifies the VXLAN gateway VTEP port profile from the VSM.

Configuring High Availability

The operation of high availability (HA) involves the following terminology:

- Cluster—A cluster is a pair of gateway modules that operate together as a single high available module. Each cluster is distinguished by a unique cluster ID. A gateway module that is deployed in a standalone mode of operation is assigned a dummy cluster ID of 0.
- HA role—The gateway modules that make up an HA cluster are assigned separate roles. One is designated as primary and the other as secondary. This role decides which of the two modules goes to active state first and which stays in a standby state. These states persist until the active fails. In the event of any failure in the active gateway module, the standby gateway detects the failure and moves to active state. This way one of the two modules is always providing active service.
- HA state— At any given time, only one gateway module from a given cluster is actively performing the gateway function. The other stays in the standby state pending the failure of the active module. A gateway module can be in the active or standby state. In addition, there is a transient initial state called the Init state. In this state, a gateway is either waiting to be assigned a role or negotiating its state with its peer.

After a gateway module is installed and brought up, the VSM assigns a role to the gateway module and can result in one of the following transitions:

- Unconfigured-Init to Standalone-Active
- Unconfigured-Init to Primary-Active
- Unconfigured-Init to Secondary-Standby
- Standalone-Active to Primary-Active
- Standalone-Active to Secondary-Active

For all other combinations, we recommend that you first fall back to the Unconfigured-Init mode using the **no service** *VXLAN Gateway module* command and then proceed to the desired role or states.

Note Roles must be preassigned to module numbers in the VSM. When a VXLAN gateway is attached to the VSM on that module, it inherits the role and state that are assigned by the VSM.

You can create a service module in a standalone mode.

Procedure

	Command or Action	Purpose
Step 1	vsm(config)# **service** *mod* **role standalone**	Configures the service module as standalone active.

	Command or Action	Purpose
Step 2	vsm(config)# **show module service-module**	Displays the service module number, cluster ID, role, HA mode and status.

This example shows how to display the cluster ID mapping and the details about active, standby, and standalone service modules:

```
vsm(config)# show module service-module
Mod  Cluster-id  Role           HA Mode       Status
---  ----------  -----------    ----------    -------
36        0      Standalone     Standalone    Active
```

You can create a service module as a high availability (HA) pair, use the following procedure:

Procedure

	Command or Action	Purpose
Step 1	vsm(config)# **service** *modNo1* **role** *primary* **ha-cluster** *clusterNo*	Configures the service module in HA and adds a primary service module to a cluster.
Step 2	vsm(config)# **service** modNo2 **role** *secondary* **ha-cluster** *clusterNo*	Configures another service module as secondary in the same cluster.
Step 3	vsm(config)# **show module service-module**	Displays the service module number, cluster ID, role, HA mode, and status.

This example shows how to display the cluster ID mapping and the details about active, standby, and standalone service modules:

```
vsm(config)# show module service-module
Mod  Cluster-id  Role        HA Mode    Status
--- ---------- ----------- ---------- -------
9    1        Primary          HA       Active
10   1        Secondary        HA       Standby
```

To switch over between the active and standby VXLAN gateway, enter the following command on the VSM:

```
vsm# service ha-cluster <1-8> switchover
```

Verifying the VXLAN Gateway Installation and Configuration

To display the VXLAN gateway (GW) installation and configuration information, perform one of the following tasks on the VSM:

Command	Purpose
show running-config port-profile gw-uplink	Displays the configuration of the port profile assigned to the VXLAN gateway uplinks.

Command	Purpose
show running-config port-profile gw-vtep	Displays the configuration of the port profile assigned to the VXLAN VTEP.
show module	Displays the VXLAN gateway service modules.
show module service-module	Verifies the role of the VXLAN gateway module and displays the cluster ID mapping and the details about active, standby, and standalone service modules.
show vxlan gateway interface	Displays if the VTEPs are configured properly.
show interface vethernet 6	Displays if both the VTEP Virtual Ethernet Interfaces are in up state.
show port-channel summary	Displays if the port channels are up for gateway service modules.
show bridge-domain mappings	Displays VLAN-VXLAN mappings configured in VSM on the Ethernet uplink port-profile of a service module/VXLAN gateway or the vEthernet access port-profile for the VXLAN trunk feature.
show switch edition	Displays if the VSM is in Advanced mode.
show feature	Displays if the VXLAN gateway is enabled on the VSM.
show virtual-service-blade summary **Note** This command needs to be executed from the Cloud Services Platform.	Displays the status of the VXLAN gateway VSB as it transitions from the VSB DEPLOY IN PROGRESS to VSB POWERED ON.
show virtual-service-blade **Note** This command needs to be executed from the Cloud Services Platform.	Displays the VXLAN gateway configuration.

This example displays the status of the VXLAN gateway VSB:

```
CSP# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                HA-Role     HA-Status   Status                    Location
--------------------------------------------------------------------------------
VXLAN-GW            PRIMARY     ACTIVE      VSB POWERED ON            PRIMARY
VXLAN-GW            SECONDARY   ACTIVE      VSB POWERED ON            SECONDARY
```

This example displays the VXLAN gateway configuration:

```
CSP# show virtual-service-blade
virtual-service-blade VXLAN-GW
```

```
  Description:
  Slot id:        1
  Host Name:      VXLAN-GW-DOCS
  Management IP:  192.168.1.104
  VSB Type Name :  vx-gw-1.5
  Configured vCPU:           3
  Operational vCPU:           3
  Configured Ramsize:        2048
  Operational Ramsize:        2048
  Disksize:       3
  Heartbeat:      154764

  Legends:   P -  Passthrough
  ---------------------------------------------------------------------------
   Interface           Type         MAC     VLAN    State   Uplink-Int
                                                   Pri  Sec Oper  Adm
  ---------------------------------------------------------------------------
  VsbEthernet1/1  gw-uplink1 0002.3d71.a303        up   up Gi3(P) Gi3(P)
  VsbEthernet1/2  management 0002.3d71.a302  751   up   up Gi1    Gi1
  VsbEthernet1/3  gw-uplink2 0002.3d71.a304        up   up Gi4(P) Gi4(P)
        internal          NA        NA       NA    up   up
  HA Role: Primary
    HA Status: ACTIVE
    Status:       VSB POWERED ON
    Location:     PRIMARY
    SW version:
  HA Role: Secondary
    HA Status: ACTIVE
    Status:       VSB POWERED ON
    Location:     SECONDARY
    SW version:
  VSB Info:
    Domain ID : 405
```

This example displays the port-profile configuration assigned to the VXLAN Gateway uplinks:

```
vsm# show running-config port-profile gw-uplink

port-profile type ethernet gw-uplink
  switchport mode trunk
  switchport trunk allowed vlan 1,81,751-760
  mtu 1550
  channel-group auto mode active
  no shutdown
  state enabled
```

This example displays the port-profile configuration assigned to the VXLAN VTEP:

```
vsm# show running-config port-profile gw-vtep

port-profile type vethernet gw-vtep
  switchport mode access
  switchport access vlan 760
  capability vxlan
  transport ip address 192.168.1.253 255.255.255.0 gateway 192.168.1.1
  no shutdown
  state enabled
```

This example shows how to display the VXLAN gateway service modules as soon as they are online:

```
vsm# show module
Mod  Ports  Module-Type                        Model               Status
---  -----  -------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    332    Virtual Ethernet Module           NA                  ok
4    332    Virtual Ethernet Module           NA                  ok
5    332    Virtual Ethernet Module           NA                  ok
6    332    Virtual Ethernet Module           NA                  ok
7    332    Virtual Ethernet Module           NA                  ok
8    332    Virtual Ethernet Module           NA                  ok
```

```
9    4      Virtual Service Module            VXLAN Gateway       ok
10   4      Virtual Service Module            VXLAN Gateway       ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    4.2(1)SV2(2.0.284)  0.0
2    4.2(1)SV2(2.0.284)  0.0
3    4.2(1)SV2(2.1)      VMware ESXi 5.0.0 Releasebuild-623860 (3.0)
4    4.2(1)SV2(2.1)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
5    4.2(1)SV2(2.1)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
6    4.2(1)SV2(2.1)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
7    4.2(1)SV2(2.1)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
8    4.2(1)SV2(2.1)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
9    4.2(1)SV2(2.1)      Linux 2.6.27.10
10   4.2(1)SV2(2.1)      Linux 2.6.27.10

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.193.81.210    NA                                    NA
2    10.193.81.210    NA                                    NA
3    10.193.81.201    3f6ebef1-90f3-11e0-a977-e8b7487bbf50  10.193.81.201
4    10.193.81.202    56ae0e11-98a8-11e0-b2a9-e8b7487c00e4  10.193.81.202
5    10.193.81.203    1abbf23b-9c26-11e0-ab53-e8b7487c26be  10.193.81.203
6    10.193.81.204    64faccd8-9c11-11e0-ba93-e8b7487c24ea  10.193.81.204
7    10.193.81.205    1abbf245-9c26-11e0-ab53-e8b7487c2712  10.193.81.205
8    10.193.81.169    0ea13991-e32f-11e0-bd1d-ccef48b424a0  10.193.81.169
9    192.168.1.104    56fa6753-4dc5-4a7d-ad07-cc817114f838  VXLAN-GW-DOCS
10   192.168.1.105    4cbd05df-b3e5-468a-9497-89aa3fae8153  VXLAN-GW-DOCS

* this terminal session
```

This example shows how to display the cluster ID mapping and the details about active, standby, and standalone service modules:

```
vsm# show module service-module
Mod  Cluster-id  Role        HA Mode    Status
--- ---------- ----------- ---------- -------
9    1        Primary          HA       Active
10   1        Secondary        HA       Standby
```

This example shows how to find the module for virtual Ethernet interface binding:

```
vsm(config-if)# show vxlan gateway interface
-----------------------------------------------------------------
Port  IPAddress  Netmask  Gateway Mod Status Role
-----------------------------------------------------------------
Veth6  192.168.1.253  255.255.255.0 192.168.1.1 9  up Active
Veth22  192.168.1.253  255.255.255.0 192.168.1.1 10  up Standby
```

This example displays if both the VTEP veths are in up state:

```
vsm# show interface vethernet 6
Vethernet6 is up
  Port description is VXLANGW VTEP, Network Adapter 1
  Hardware: Virtual, address: 0002.3d71.a303 (bia 0002.3d71.a303)
  Owner is VM "VXLANGW VTEP", adapter is Network Adapter 1
  Active on module 9
  Port-Profile is gw-vtep
  Port mode is access
  5 minute input rate 8 bits/second, 0 packets/second
  5 minute output rate 0 bits/second, 0 packets/second
  Rx
    6 Input Packets 6 Unicast Packets
    0 Multicast Packets 588 Broadcast Packets
    468 Bytes
  Tx
    34321 Output Packets 34321 Unicast Packets
    33609 Multicast Packets 24 Broadcast Packets 33633 Flood Packets
    2193700 Bytes
    0 Input Packet Drops 0 Output Packet Drops

vsm# show interface vethernet 22
Vethernet22 is up
  Port description is VXLANGW VTEP, Network Adapter 1
```

```
  Hardware: Virtual, address: 0002.3d71.a383 (bia 0002.3d71.a383)
  Owner is VM "VXLANGW VTEP", adapter is Network Adapter 1
  Active on module 10
  Port-Profile is gw-vtep
  Port mode is access
  5 minute input rate 8 bits/second, 0 packets/second
  5 minute output rate 0 bits/second, 0 packets/second
  Rx
    6 Input Packets 6 Unicast Packets
    0 Multicast Packets 25 Broadcast Packets
    468 Bytes
  Tx
    33742 Output Packets 33742 Unicast Packets
    33609 Multicast Packets 133 Broadcast Packets 33742 Flood Packets
    2158956 Bytes
    0 Input Packet Drops 0 Output Packet Drops
```

This example displays if port-channels are up for gateway service modules:

```
vsm# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(SU)     Eth      NONE      Eth3/3(P)    Eth3/4(P)    Eth3/5(P)
                                     Eth3/6(P)
2     Po2(SU)     Eth      NONE      Eth4/3(P)    Eth4/4(P)    Eth4/5(P)
                                     Eth4/6(P)
3     Po3(SU)     Eth      NONE      Eth5/3(P)    Eth5/4(P)    Eth5/5(P)
                                     Eth5/6(P)
4     Po4(SU)     Eth      NONE      Eth6/3(P)    Eth6/4(P)    Eth6/5(P)
                                     Eth6/6(P)
5     Po5(SU)     Eth      NONE      Eth7/3(P)    Eth7/4(P)    Eth7/5(P)
                                     Eth7/6(P)
6     Po6(SU)     Eth      NONE      Eth8/4(P)
7     Po7(SU)     Eth      LACP      Eth9/1(P)    Eth9/3(P)
8     Po8(SU)     Eth      LACP      Eth10/1(P)   Eth10/3(P)
```

This example shows VXLAN gateway mappings:

```
vsm# show bridge-domain mappings
--------------------------------------------------------------------------------
Interface       Module  Serv Inst  Vlan  BD-Name
--------------------------------------------------------------------------------
port-channel7   9       753        753   bd-753
port-channel8   10      753        753   bd-753
```

Note The value in the Interface column varies based on the VXLAN gateway or the VXLAN trunk feature. Vethernet<number> in the Interface column indicates mapping for the VXLAN trunk feature; port-channel<number> in the Interface column indicates mapping configured on the VXLAN gateway.

This example shows how to find the IP address for module binding:

```
vsm(config-if)# show service-module mgmt-int
 --------------------------------------------------------------------------------
Mod Interface-Name IP-address Speed MTU
--------------------------------------------------------------------------------
4 Mgmt0 10.10.10.2             0     0
5 Mgmt0 10.10.10.3             0     0
Remember the management IP address user installs gateway with
(in this example 10.10.10.2, which occupies module slot 4)
```

This example shows how to display if the VSM is in Advanced mode:

```
vsm# show switch edition
Switch Edition: Advanced

Advanced Features
Feature Name    Feature State
----------------------------
vxlan-gateway   enabled

Licenses Available: 1020
Licenses In Use: 4
License Expiry Date: 13 Jun 2013
```

This example shows if the VXLAN gateway is enabled on the VSM:

```
vsm# show feature
Feature Name          Instance  State
--------------------  --------  --------
cts                   1         enabled
dhcp-snooping         1         enabled
http-server           1         enabled
lacp                  1         enabled
netflow               1         disabled
network-segmentation  1         enabled
port-profile-roles    1         disabled
private-vlan          1         enabled
segmentation          1         enabled
sshServer             1         enabled
tacacs                1         disabled
telnetServer          1         disabled
vtracker              1         enabled
vxlan-gateway         1         enabled
```

Perform one of the following tasks on the VXLAN gateway. If your VSM is on Layer 3 through management and your gateway is also on the same management subnet, use the **attach module** < *service module number*> command to acces the gateway CLI. If your VSM is on Layer 3 through control, you can access the gateway CLI from any machine on that control subnet. For this example, we are using the VSM which is on L3 control.

Command	Purpose
show redundancy config	Displays the high availability status.

This example displays the high availability status:

```
gw# show redundancy config

HA Manager Node Information:

    Cluster Node Count: 2

    Local Node:
      state          : Active
      HA mode        : High Availability
      uuid           : 56fa6753-4dc5-4a7d-ad07-cc817114f838
      cluster_id     : 1
      node_priority  : 2
      node_type      : VXLAN Gateway
      ipaddr [mgmt]  : 192.168.1.104

    Peer Node 1:
      state          : Standby
      uuid           : 4cbd05df-b3e5-468a-9497-89aa3fae8153
      node_type      : VXLAN Gateway
      ipaddr [mgmt]  : 192.168.1.105
```

Managing the VXLAN to VLAN Mappings on the VXLAN Gateway

The VLAN to VXLAN mappings that are configured on a gateway module can be managed by editing the port profile applied on the gateway uplink modules. To add or remove a mapping, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	vsm(config)# **port-profile** *port-profile-name*	Specifies the name of the port-profile applied to gw-uplink1 and gw-uplink2 in Installing a VXLAN Gateway as a Virtual Service Blade.
Step 2	vsm(config-port-prof)# **service instance** *1 to 4096*	Defines a place holder for mappings. The range is from 1 to 4096. **Note** Port profiles that contain the **service instance** keyword cannot be used for a non-VXLAN gateway module.
Step 3	vsm(config-port-prof-srv)# **encapsulation dot1q** *1-4094* **bridge-domain** *name*	Adds a new mapping.
Step 4	vsm(config-port-prof-srv)# no **encapsulation dot1q** *1-4094* **bridge-domain** *name*	Deletes an existing mapping.

This example shows how to configure VXLAN to VLAN mappings on the VXLAN gateway:

```
vsm(config)# show run port-profile Uplink-All-VXGW
port-profile type ethernet Uplink-All-VXGW
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 1545-1575,1577-1605
  mtu 1550
  service instance 2
    encapsulation dot1q 1557 bridge-domain vxlan6002
    encapsulation dot1q 1555 bridge-domain vxlan6000
    encapsulation dot1q 1558 bridge-domain vxlan6003
    encapsulation dot1q 1559 bridge-domain vxlan6004
     channel-group auto mode active
  no shutdown
  state enabled
vsm(config)# show port-profile usage
port-profile Uplink-All-VXGW
 port-channel1
 port-channel5
 Ethernet7/1
 Ethernet7/3
vsm(config)# show run interface ethernet 7/1 expand-port-profile
interface Ethernet7/1
  switchport mode trunk
  switchport trunk allowed vlan 1545-1575,1577-1605
  mtu 1550
  channel-group auto mode active
  service instance 2
    no shutdown
    encapsulation dot1q 1557 bridge-domain vxlan6002
    encapsulation dot1q 1555 bridge-domain vxlan6000
```

```
encapsulation dot1q 1558 bridge-domain vxlan6003
no shutdown
```

Deleting the VXLAN Gateway

To delete the VXLAN gateway from the Cloud Services Platform, use the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters the global configuration mode on the Cloud Services Platform.
Step 2	csp(config)# **virtual-service-blade** *<vsb name>*	Enters into the virtual-service-blade sub-command.
Step 3	csp(config-vsb-config)# **shutdown**	Shuts down the virtual-service-blade.
Step 4	csp(config)# **no virtual-service-blade** *<vsb name>*	Deletes the virtual-service-blade from the Cloud Services Platform.

To delete the VXLAN gateway from the VSM, use the following procedure:

Note You need to remove the associated VEM and port-channel information associated with the VXLAN gateway VSB.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters the global configuration mode on the Cloud Services Platform.
Step 2	vsm(config)# **no vem** *<vem number associated with the primary vxlan-gw VSB>*	Deletes the unused VEM associated with the deleted primary VXLAN gateway.
Step 3	vsm(config)# **no vem** *<vem number associated with the secondary vxlan-gw VSB>*	Deletes the unused VEM associated with the deleted secondary VXLAN gateway.
Step 4	vsm(config)# **no interface port-channel** *<po number associated with the primary vxlan-gw VSB>*	Deletes the unused port-channel interface associated with the deleted primary VXLAN gateway VEM.

	Command or Action	Purpose
Step 5	vsm(config)# **no interface port-channel** *<po number associated with the secondary vxlan-gw VSB>*	Deletes the unused port-channel interface associated with the deleted secondary VXLAN gateway VEM.

Feature History for VXLAN Gateways

Feature Name	Releases	Feature Information
VXLAN Gateway	4.2(1)SV2(2.1)	Introduced the Virtual Extensible Local Area Network (VXLAN) gateway feature.

CHAPTER 4

Configuring Advanced Features

This chapter contains the following sections:

VXLAN trunk is used to configure ports that can individually map a .1Q tag value to a VXLAN. Ports receive the packets with the .1Q tag and are used in mapping the packet into a VXLAN. You can use the VXLAN trunk feature to support network service VMs which need access to more VXLANs than the number of VNICs VMware supports on a VM.

- Configuring VXLAN Trunks, page 41
- Configuring Multi-MAC Capability, page 42

Configuring VXLAN Trunks

You can trunk multiple VXLANs on a single vEthernet interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile type vethernet** *name*	Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics: • **name—**The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V. • **type—**(Optional) The port profile type can be Ethernet or vEthernet.
Step 3	switch(config -port-profile)# **switchport access bridge-domain** *name-string*	Assigns a VXLAN bridge domain to this profile for non-dot1q traffic.

	Command or Action	Purpose
Step 4	switch(config -port-profile)# [**no**] **service instance** *1 to 4096*	Defines a place holder for mappings. The range is from 1 to 4096.
Step 5	switch(config -port-profile)# [**no**] **encapsulation dot1q** *1-4094* **bridge-domain** *name*	Creates mappings. The range is from 1 to 4094.

This example shows how to configure a VXLAN trunk:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# port-profile type vethernet csr-access
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access bridge-domain bd-701
switch(config-port-prof)# service instance 10
switch(config-port-prof-srv)# encapsulation dot1q 600 bridge-domain bd-600
switch(config-port-prof-srv)# encapsulation dot1q 601 bridge-domain bd-601
switch(config-port-prof-srv)# encapsulation dot1q 602 bridge-domain bd-602
switch(config-port-prof-srv)# no shutdown
cswitch(config-port-prof-srv)# state enabled
switch(config-port-prof)# end
switch# show run port-profile csr-access
port-profile type vethernet csr-access
  switchport mode access
  switchport access bridge-domain bd-701
  service instance 10
    encapsulation dot1q 600 bridge-domain bd-600
    encapsulation dot1q 601 bridge-domain bd-601
    encapsulation dot1q 602 bridge-domain bd-602
  state enabled
```

This example shows how to display VXLAN trunk interface mappings:

```
switch(config-bd)# show bridge-domain mappings

--------------------------------------------------------------------------------
Interface      Service Instance ID      Module ID    Vlan ID      Segment ID
--------------------------------------------------------------------------------
Vethernet2                 10            3            600            5000
Vethernet2                 10            3            601            5001
Vethernet2                 10            3            602            5002

switch(config-bd)#
```

Note The value in the Interface column varies based on the VXLAN gateway or the VXLAN trunk feature. Vethernet<number> in the Interface column indicates mapping for the VXLAN trunk feature; port-channel<number> in the Interface column indicates mapping configured on the VXLAN gateway.

Configuring Multi-MAC Capability

You can mark a virtual Ethernet interface as capable of sourcing packets from multiple MAC addresses.

Before You Begin

Do not use the multi-MAC capability feature if MAC distribution (segment distribution MAC) is enabled.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile type vethernet** *name*	Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics: • **name—**The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V. • **type—**(Optional) The port profile type can be Ethernet or vEthernet.
Step 3	Switch(config)# [**no**] **capability multi- mac**	Marks the vEthernet port as multi-MAC capable.

This example shows how to configure the multi-MAC capability feature:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-port-prof)# port-profile type vethernet csr-multi-mac-access
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access bridge-domain bd-701
switch(config-port-prof)# capability multi-mac
switch(config-port-prof)# state enabled
switch(config-port-prof)# no shutdown
switch(config-port-prof)# end
switch# show running-config port-profile csr-multi-mac-access
port-profile type vethernet csr-multi-mac-access
  switchport mode access
  switchport access bridge-domain bd-701
  capability multi-mac
  no shutdown
  state enabled
```

CHAPTER 5

Upgrading VXLAN Gateway from VSM

This chapter contains the following sections:

- Upgrading VXLAN Gateway Service Module, page 45
- Upgrading VXLAN Gateway Cluster, page 46

Upgrading VXLAN Gateway Service Module

You can upgrade a VXLAN gateway service module (standalone) from the VSM by using the kickstart and system image or the iso image.

Note During the upgrade process, the VXLAN gateway service module is reloaded. Therefore, the VXLAN gateway service module may be unavailable for few minutes which can impact the datapath traffic.

Before You Begin

Ensure the following:

- The VXLAN gateway module is attached to the VSM.
- The VXLAN gateway module is configured in the standalone mode. For information about configuring the standalone mode, see Configuring High Availability, on page 31.

Procedure

	Command or Action	Purpose
Step 1	vsm# **install service-module kickstart bootflash:** *kickstart image* **system bootflash:** *system image* **module-num** *3–130*	Upgrades the VXLAN gateway service module by using the kickstart and system image. The module number range is from 3 to 130.

	Command or Action	Purpose
Step 2	vsm# **install service-module iso bootflash:** *iso image* **module-num** *3–130*	Upgrades the VXLAN gateway service module by using the iso image. The module number range is from 3 to 130.

Upgrading VXLAN Gateway Cluster

You can upgrade a VXLAN gateway high availability (HA) cluster from the VSM by using the kickstart and system image or the iso image. To ensure that at least one VXLAN gateway service module within a cluster is available to serve the datapath traffic during an upgrade, the service modules within a cluster are upgraded in the following sequence:

1. The VXLAN gateway standby service module is upgraded.

   After the VXLAN gateway standby module is upgraded and it is online, it forms the HA cluster with the VXLAN gateway active service module.

2. The VXLAN gateway active service module is upgraded so that the standby service module can serve the datapath traffic.

Note If the standby service module fails to form HA in step 1, the active service module is still upgraded to maintain uniform software version in the cluster. In such a case, the datapath traffic is impacted.

Before You Begin

Ensure the following:

- The VXLAN gateway modules are attached to the VSM.
- The VXLAN gateway modules are configured in the HA mode. For information about configuring the HA mode, see Configuring High Availability, on page 31.

Procedure

	Command or Action	Purpose
Step 1	vsm# **install service-module kickstart bootflash:** *kickstart image* **system bootflash:** *system image* **cluster-id** *1–8*	Upgrades the VXLAN gateway cluster by using the kickstart and system image. The cluster ID range is from 1 to 8.
Step 2	vsm# **install service-module iso bootflash:** *iso image* **cluster-id** *1–8*	Upgrades the VXLAN gateway cluster by using the iso image. The cluster ID range is from 1 to 8.

INDEX

C

configuring 25
    VXLAN 25
        Termination 25
Configuring 31, 38
    High 31
        Availability 31
    VXLAN 38
        VLAN 38
            Mappings 38
creating 12, 14
    a port profile configured to use a VXLAN 14
    VXLANs 12

D

default settings 9
    VXLANs 9
deleting 17
    VXLANs 17
disabling 17
    segmentation 17

E

enabling 9
    VXLANs 9

F

feature disabled 5
feature history 20, 40
    VXLAN 20, 40
        Gateway 40
fragmentation 4

J

jumbo frames 5

O

overview 1
    VXLANs 1

P

prerequisites 7
    VXLAN 7

R

removing 16
    ports from a VXLAN 16

S

segmentation 17
    disabling 17

U

Upgrading 45
    VXLAN 45
        Gateway 45

V

VEM 3
    L3 IP Interface for VXLAN 3

verifying 19
VXLAN configuration 19
verifying the 32
VXLAN 32
Gateway 32
Installation 32
Configuration 32
Virtual 27
Service 27
Blade 27
vmknics 10
configuring for encapsulation 10
VXLAN 3, 27
Gateway 3, 27
VXLAN offload 5
VXLANs 1, 4, 9, 12, 17
creating 12
default settings 9
deleting 17
enabling 9
initial enabling 9
maximum number 4
overview 1