Send document comments to nexus1k-docfeedback@cisco.com.

Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)

April 18, 2012

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-25747-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

*In*ternet Protocol (IP) addresses and phone numbers that are used in the examples, command display output, and figures within this document are for illustration only. If an actual IP address or phone number appears in this document, it is coincidental.

Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)
© 2012 Cisco Systems, Inc. All rights reserved.

Send document comments to nexus1k-docfeedback@cisco.com.

Send document comments to nexus1k-docfeedback@cisco.com.

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1).* The preface also provides information on how to obtain related documentation.

This preface includes the following sections:

Audience

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

- An understanding of the Cisco Nexus 1000

Note Note: Knowledge of VMware vNetwork Distributed Switch is not a prerequisite.

Document Organization

This publication is organized into the following chapters:

Chapter and Title	Description
Chapter 1, “Overview”	Provides an overview of VXLAN.
Chapter 2, “Configuring VXLAN”	Describes the basic VXLAN configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
{ }	Elements in braces are required choices.
[ ]	Elements in square brackets are optional.
x | y | z	Alternative, mutually exclusive elements are separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

`screen font`	Terminal sessions and information the device 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 for notes and cautions:

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.

Recommended Reading

Before configuring the Cisco Nexus 1000V, we recommend that you read and become familiar with the following documentation:

- *Cisco Nexus 1000V Network Segmentation Manager Configuration Guide, Release 4.2(1)SV1(5.1)*

Send document comments to nexus1k-docfeedback@cisco.com.

Related Documentation

This section lists the documents used with the Cisco Nexus 1000 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, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)

Cisco Nexus 1010 Management Software Release Notes, Release 4.2(1)SP1(3)

Install and Upgrade

Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide

Cisco Nexus 1010 Software Installation and Upgrade Guide, Release 4.2(1)SP1(3)

Configuration Guides

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Network Segmentation Manager Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(3)

Programming Guide

Cisco Nexus 1000V XML API User Guide, Release 4.2(1)SV1(5.1)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V MIB Quick Reference

Cisco Nexus 1010 Command Reference, Release 4.2(1)SP1(3)

Send document comments to nexus1k-docfeedback@cisco.com.

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(5.1)

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

Virtual Security Gateway Documentation

Cisco Virtual Security Gateway for Nexus 1000V Series Switch

Virtual Network Management Center

Cisco Virtual Network Management Center

Network Analysis Module Documentation

Cisco Prime Network Analysis Module Software Documentation Guide, 5.1

Cisco Prime Network Analysis Module (NAM) for Nexus 1010 Installation and Configuration Guide, 5.1

Cisco Prime Network Analysis Module Command Reference Guide 5.1

Cisco Prime Network Analysis Module Software 5.1 Release Notes

Cisco Prime Network Analysis Module Software 5.1 User Guide

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Send document comments to nexus1k-docfeedback@cisco.com.

CHAPTER 1

Overview

This chapter provides an overview of Virtual Extensible Local Area Network (VXLAN).

This chapter includes the following sections:

Information About VXLAN

Overview

The VXLAN creates LAN segments by using an overlay approach with MAC in IP encapsulation. The encapsulation carries the original Layer 2 (L2) frame from the Virtual Machine (VM) which is encapsulated from within the Virtual Ethernet Module (VEM). Each VEM is assigned an IP address which is used as the source IP address when encapsulating MAC frames to be sent on the network. You can have multiple vmknics per VEM that are used as sources for this encapsulated traffic. The encapsulation carries the VXLAN identifier which is used to scope the MAC address of the payload frame.

The connected VXLAN is indicated within the port profile configuration of the vNIC and is applied when the VM connects. Each VXLAN uses an assigned IP multicast group to carry broadcast traffic within the VXLAN segment.

When a VM attaches to a VEM, if it is the first to join the particular VXLAN segment on the VEM, an IGMP Join is issued for the VXLAN's assigned multicast group. When the VM transmits a packet on the network segment, a lookup is made in the L2 table using the destination MAC of the frame and the VXLAN identifier. If the result is a hit, the L2 table entry will contain the remote IP address to use to encapsulate the frame and the frame will be transmitted within an IP packet destined to the remote IP address. If the result is a miss (broadcast/multicast/unknown unicasts fall into this bucket), the frame is encapsulated with the destination IP address set to be the VXLAN segment's assigned IP multicast group.

Send document comments to nexus1k-docfeedback@cisco.com.

When an encapsulated packet is received from the network, it is decapsulated and the source MAC address of the inner frame and VXLAN ID, is added to the L2 table as the lookup key and the source IP address of the encapsulation header will be added as the remote IP address for the table entry.

VEM L3 IP Interface for VXLAN

When a VEM has a vEthernet interface connected to a VXLAN, the VEM requires at least one IP/MAC pair to terminate VXLAN packets. In this regard, the VEM acts as an IP host. The VEM only supports IPv4 addressing for this purpose.

Similar to how the VEM L3 Control is configured, the IP address to use for VXLAN is configured by assigning a port profile to a vmknic that has the **capability vxlan** command in it.

To support carrying VXLAN traffic over multiple uplinks , or sub-groups, in server configurations where vPC-HM MAC-Pinning is required, up to four vmknics with **capability vxlan** may be configured. We recommend that all the VXLAN vmknics within the same ESX/ESXi host are assigned to the same port profile which must have the **capability vxlan** parameter.

VXLAN traffic sourced by local vEthernet interfaces is distributed between these vmknics based on the source MAC in their frames. The VEM automatically pins the multiple VXLAN vmknics to separate uplinks. If an uplink fails, the VEM automatically repins the vmknic to a working uplink.

When encapsulated traffic is destined to a VEM connected to a different subnet, the VEM does not use the VMware host routing table. Instead, the vmknic initiates an ARP for the remote VEM IP addresses. The upstream router must be configured to respond by using the Proxy ARP feature.

Fragmentation

The VXLAN encapsulation overhead is 50 bytes. In order to prevent performance degradation due to fragmentation, the entire interconnection infrastructure between all VEMs exchanging VXLAN packets should be configured to carry 50 bytes more than what the VM VNICs are configured to send. For example, using the default VNIC configuration of 1500 bytes, the VEM uplink port profile, upstream physical switch port, and interswitch links, and any routers if present, must be configured to carry an MTU of at least 1550 bytes. If that is not possible, it is suggested that the MTU within the guest VMs be configured to be smaller by 50 bytes, For example, 1450 bytes.

If this is not configured, 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 only occurs at the IP layer. If the VM sends a frame that is too large to carry, after adding the VXLAN encapsulation, and the frame does not contain an IP packet, the frame is dropped.

Scalability

Maximum Number of VXLANs

The Cisco Nexus 1000V supports a total of 2048 VLANs and/or VXLANs. Either 2048 VLANs or 2048 VXLANs, or any combination adding to no more than 2048. This number matches up with the maximum number of ports on the Cisco Nexus 1000V. Thereby, allowing every port to be connected to a different VLAN or VXLAN.

Send document comments to nexus1k-docfeedback@cisco.com.

Supported Features

This section contains the following topics:

Jumbo Frames

Jumbo frames are supported by the Cisco Nexus 1000V to the extent that there is room leftover to accommodate the VXLAN encapsulation overhead, of at least 50 bytes, and the physical switch/router infrastructure can transport these jumbo sized IP packets.

Disabling the VXLAN Feature Globally

As a safety precaution, the **no feature segmentation** command will not be allowed if there are any ports associated with a VXLAN port profile. You must remove all the associations before disabling the feature. The **no feature segmentation** command will cleanup all the VXLAN Bridge Domain configurations on the Cisco Nexus 1000V.

Send document comments to nexus1k-docfeedback@cisco.com.

Send document comments to nexus1k-docfeedback@cisco.com.

CHAPTER 2

Configuring VXLAN

This chapter describes how to configure the Virtual Extensible Local Area Network (VXLAN).

This chapter includes the following topics:

Information About VXLAN

For detailed information about VXLAN, see Chapter 1, “Overview”.

Prerequisites for VXLAN

VXLAN has the following prerequisites:

- The Cisco Nexus 1000V uplink port profiles and all interconnecting switches/routers in between the ESX hosts must have their supported MTU set to at least 50 bytes larger than the MTU of the VMs. For example, the VMs default to using a 1500 byte MTU (same as the uplinks and physical devices), so in this case they must be set to at least 1550 bytes. If this isn’t possible, then all VM’s VNICs should have their MTU lowered to be 50 bytes smaller than what the physical network supports, for example 1450 bytes. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*.
- If the Cisco Nexus 1000V is using a port channel for its uplinks, then the load distribution algorithm should be set to use a 5-tuple hash (IP/L4/L4 Ports). The same should be used for any port channels on the physical switches. For more information, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*.
- If VEMs requiring VXLAN connectivity are separated by a router
  - Proxy ARP must be enabled on the SVIs connected to the Cisco Nexus 1000V’s VXLAN transport VLANs (the ones the “capability vxlan” port profiles are connected to).
  - Multicast routing must be enabled on the routers.

Send document comments to nexus1k-docfeedback@cisco.com.

- VXLAN makes use of MAC in IP (UDP) with a destination port of 8472. You must allow this through any firewall.
- Your upstream switch, from the VEMs of the Cisco Nexus 1000V, needs to provide an IGMP querier function.

Default Settings

Table 2-1 lists the default settings for VXLAN parameters.

Table 2-1 Default VXLAN Parameters

Parameters	Default
VXLAN	Disabled

Configuring VXLAN

This section includes the following topics:

Initial Enabling of VXLANs

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

Configuring vmknics for VXLAN Encapsulation

You can configure vmknics for VXLAN encapsulation by running the following procedure.

BEFORE YOU BEGIN

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

SUMMARY STEPS

1. **configure terminal**
2. **port-profile** *profilename*

Send document comments to nexus1k-docfeedback@cisco.com.

3. **vmware port-group** *name*
4. **switchport mode access**
5. **switchport access vlan** *id*
6. **capability vxlan**
7. **no shutdown**
8. **state enabled**
9. **show port-profile name** *profilename*
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**port-profile** *profilename*
	
	Example:
	`switch(config)# port-profile vmknic-pp`
	`switch(config-port-prof)`
		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	**vmware port-group** *name*
	
	Example:
	`switch(config-port-prof)# vmware port-group`
	`switch(config-port-prof)#`
		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 the vCenter Server.

Step 4	**switchport mode access**
	
	Example:
	`switch(config-port-prof)# switchport mode access`
	`switch(config-port-prof)#`
		Designates the interfaces as switch access ports (the default).

Step 5	**switchport access vlan** *id*
	
	Example:
	`switch(config-port-prof)# switchport access vlan 100`
	`switch(config-port-prof)`
		Assigns a VLAN ID to this port profile.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose

Step 6	**capability vxlan**
	
	Example:
	`switch(config-port-prof)# capability vxlan`
	`switch(config-port-prof)`
		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	**no shutdown**
	
	Example:
	`switch(config-port-prof)# no shutdown`
	`switch(config-port-prof)`
		Administratively enables all ports in the profile.

Step 8	**state enabled**
	
	Example:
	`switch(config-port-prof)# state enabled`
	`switch(config-port-prof)`
		Sets the operational state of a port profile.

Step 9	**show port-profile name** *profilename* **Example:** `switch# show port-profile vmknic-pp`	(Optional) Displays the port profile configuration.
Step 10	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

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.

Enabling VXLANs

You can enable VXLANs by performing the following procedure.

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 later. If the feature level is not 4.2(1)SV1(5.1) or later, see the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(5.1)*.

SUMMARY STEPS

1. **configure terminal**
2. **feature segmentation**
3. **show feature | grep segmentation**
4. **show processes | grep seg_bd**
5. **copy running-config startup-config**

Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.

Step 2	**feature segmentation**
	
	Example:
	switch(config)# feature segmentation
	switch(config)
		Enables the VXLAN feature.

Step 3	**show feature | grep segmentation** **Example:** switch# show feature | grep segmentation	(Optional) Displays if the VXLAN feature is enabled.
Step 4	**show processes | grep seg_bd** **Example:** switch# show processes | grep seg_bd	(Optional) Displays if the VXLAN process is running.
Step 5	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

EXAMPLES

The following example shows enabling the segmentation feature.

```
n1000v# configure terminal
n1000V(config)# feature segmentation
n1000v(config)# show feature | grep segmentation
network-segmentation 1 disabled
segmentation         1 enabled
n1000v(config)# show processes | grep seg_bd
4166    S  b7de9468            1      - seg_bd
n1000v(config)# copy running-config startup-config
```

Creating a VXLAN

You can create a VXLAN by running the following procedure.

RESTRICTIONS

- You are limited to creating a combination of 2048 VXLANs and VLANs.

SUMMARY STEPS

1. **configure terminal**
2. **bridge-domain** *name-string*
3. **segment id** [*number*]
4. **group** *ipaddr*

Send document comments to nexus1k-docfeedback@cisco.com.

5. **show bridge-domain** *name-string*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**bridge domain** *name-string*
	
	Example:
	`switch(config)# bridge-domain tenant-red`
	`switch(config-bd)#`
		Creates a VXLAN and associates an identifying name to it.

Step 3	**segment id [***number***]**
	
	Example:
	`switch(config-bd)# segment id 20480`
	`switch(config-bd)#`
		Specifies the VXLAN Segment ID. Only one Bridge Domain can use a particular segment id value.
		
		Valid values are 4096 to 16777215. (1 - 4095 are reserved for VLANs.)

Step 4	**group** *ipaddr*
	
	Example:
	`switch(config-bd)# group 239.1.1.1`
	`switch(config-bd)#`
		Associates the multicast group for broadcasts and floods.
		
		Note Reserved multicast addresses are not allowed.

Step 5	**show bridge-domain** *name-string*
	
	Example:
	`switch# show bridge-domain tenant-red`
	`switch(config-bd)#`
		(Optional)

Step 6	**copy running-config startup-config**
	
	Example:
	`switch(config-bd)#`
	`copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Creating a Port Profile Configured to Use a VXLAN

You can create a port profile that is configured to use a VXLAN.

RESTRICTIONS

- Alternatively, you can associate ports with a bridge domain by modifying the configuration of an existing vEthernet 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.

SUMMARY STEPS

1. **configure terminal**
2. **port-profile** *profilename*

Send document comments to nexus1k-docfeedback@cisco.com.

3. **vmware port-group** *name*
4. **switchport mode access**
5. **switchport access bridge-domain** *name-string*
6. **no shutdown**
7. **state enabled**
8. **show port-profile name** *profilename*
9. **show running-config bridge-domain**
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.

Step 2	**port-profile** *profilename*
	
	Example:
	switch(config)# port-profile tenant-profile
	switch(config-port-prof)
		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, then it cannot be used to configure VMware virtual ports.

Step 3	**vmware port-group** *name* **Example:** switch(config-port-prof)# vmware port-group switch(config-port-prof)#	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 the vCenter Server.

Step 4	**switchport mode access**
	
	Example:
	switch(config-port-prof)# switchport mode access
	switch(config-port-prof)
		Designates the interfaces as switch access ports (the default).

Step 5	**switchport access bridge-domain** *name-string*
	
	Example:
	switch(config-port-prof)# switchport access bridge-domain tenant-red
	switch(config-port-prof)
		Assigns a VXLAN bridge domain to this port profile.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose

Step 6	**no shutdown**
	
	Example:
	`switch(config-port-prof)# no shutdown`
	`switch(config-port-prof)#`
		Administratively enables all ports in the profile.

Step 7	**state enabled**
	
	Example:
	`switch(config-port-prof)# state enabled`
	`switch(config-port-prof)`
		Sets the operational state of a port profile.

Step 8	**show port-profile name** *profilename* **Example:** `switch(config-port-prof) # show port-profile name tenant-profile`	(Optional) Displays the configuration of a port profile.
Step 9	**show running-config bridge-domain** **Example:** `switch(config-port-prof) # show running-config bridge-domain`	(Optional) Displays the segmentation configuration.
Step 10	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Removing Ports from a VXLAN

You can remove ports from a VXLAN by executing the following procedure.

RESTRICTIONS

- Executing this procedure moves the ports to the default VLAN.

SUMMARY STEPS

1. **configure terminal**
2. **port-profile** *name*
3. **no switchport access bridge-domain**
4. **show port-profile usage**
5. **show bridge-domain** *name*
6. **copy running-config startup-config**

Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**port-profile** *name*
	
	Example:
	`switch(config)# port-profile tenant-profile`
	`switch(config-port-prof)`
		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.
		Note If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.

Step 3	**no switchport access bridge-domain**
	
	Example:
	`switch(config-port-prof)# no switchport access bridge-domain tenant-red`
	`switch(config-port-prof)`
		Removes the VXLAN bridge domain from this port profile.

Step 4	**show port-profile usage** **Example:** `switch# show port-profile usage`	(Optional) Displays a list of interfaces that inherited a port profile.
Step 5	**show bridge-domain** **Example:** `switch# show bridge-domain`	(Optional) Displays all bridge domains.
Step 6	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Deleting a VXLAN

You can delete a VXLAN domain by executing the following procedure.

RESTRICTIONS

- Deleting an existing bridge domain with ports on it moves all the ports to a **down** state. Traffic stops flowing.

SUMMARY STEPS

1. **configure terminal**
2. **no bridge-domain** *name-string*
3. **show bridge-domain**

Send document comments to nexus1k-docfeedback@cisco.com.

4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no bridge-domain** *name-string*
	
	Example:
	`switch(config)# no bridge-domain group-red`
	`switch(config-bd)`
		Deletes a VXLAN.

Step 3	**show bridge-domain** **Example:** `switch# show bridge-domain`	(Optional) Displays all bridge domains.
Step 4	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Disabling Segmentation

You can disable segmentation by executing the following procedure.

SUMMARY STEPS

1. **configure terminal**
2. **show bridge-domain**
3. **show running-config port-profile**
4. **port-profile** *name*
5. **no switchport access bridge-domain** *name-string*
6. **show port-profile usage**
7. **show bridge-domain** *name*
8. **no feature segmentation**
9. **show processes | grep seg_bd**
10. **copy running-config startup-config**

Send document comments to nexus1k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**show bridge-domain**
	
	Example:
	`switch(config)# show bridge-domain`
	`switch(config)#`
		Displays all bridge domains.
		
		Note You must identify all bridge domains with non-zero port counts.

Step 3	**show running-config port-profile** **Example:** `switch(config)# show running port-profile`	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	**port-profile** *name*
	
	Example:
	`switch(config)# port-profile tenant-profile`
	`switch(config-port-prof)`
		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:
		• *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, then it cannot be used to configure VMware virtual ports.

Step 5	**no switchport access bridge-domain** *name-string*
	
	Example:
	`switch(config-port-prof)# no switchport access bridge-domain tenant-red`
	`switch(config-port-prof)`
		Removes the VXLAN bridge domain from this port profile.

Step 6	**show port-profile usage** **Example:** `switch# show port-profile usage`	(Optional) Displays a list of interfaces that inherited a port profile.
Step 7	**show bridge-domain** **Example:** `switch# show bridge-domain`	(Optional) Displays all bridge domains.

Step 8	**no feature segmentation**
	
	Example:
	`switch(config)# no feature segmentation`
	`switch(config)#`
		Removes the segmentation feature.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 9	**show processes | grep seg_bd** **Example:** switch(config)# show processes | grep seg_bd switch(config)#	Displays the processes to determine that the segmentation feature is not running.
Step 10	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Verifying VXLAN Configuration

To display VXLAN configuration information, enter one of the following commands:

Command	Purpose
show processes | grep seg_bd	Displays that the VXLAN process is running.
show bridge-domain	Displays all bridge domains.
show interface brief	Displays a short version of the interface configuration.
show interface switchport	Displays information about switchport interfaces.

EXAMPLES

This example shows how to display if the VXLAN process is running.

```
switch (config)# show processes | grep seg_bd
    -     NR       -            1     - seg_bd
```

This example shows how to display all bridge domains.

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

Bridge-domain tenant-red (2 port in all)
Segment ID: 5000 (manual/Active
Group IP: 239.1.1.1
    -     NR       -            1     - seg_bd
```

This example shows how to display a short version of the interface table.

```
switch(config)# show interface brief

--------------------------------------------------------------------------------
Port      VRF     Status   IP Address                    Speed      MTU
--------------------------------------------------------------------
mgmt 0    --      up       172.23.233.117                1000       1500

--------------------------------------------------------------------------------
Ethernet     VLAN   Type Mode   Status  Reason          Speed    Port
Interface                                               Ch #
--------------------------------------------------------------------------------
Eth3/5       1      eth  trunk  up      none            1000

--------------------------------------------------------------------------------
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
Vehternet   VLAN   Type Mode   Status  Reason         Speed
------------------------------------------------------------------------
Veth1       --     virt access up      none           auto
Veth1       --     virt access up      none           auto
Veth1       100    virt access up      none           auto

------------------------------------------------------------------------
Port     VRF    Status   IP Address                     Speed      MTU
control0 --     up       --                             1000       1500
switch#(config)#
```

This example shows how to display information about switchport interfaces.

```
switch#(config)# show int switchport
Name: Ethernet3/5
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: Trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode: trunk
  Trunking VLANs Enabled: 180-181,231-233,571-574
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs:
  Operational private-vlan: none

ifindex 0x1c000000 swbd 4096
Name Vethernet1
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 0 (none)
  Access BD name: tenant-red
  Trunking Native ModeVLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs:
  Operational private-vlan: none
```

For detailed information about the fields in the output from these commands, refer to the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*.

Send document comments to nexus1k-docfeedback@cisco.com.

Feature History for VXLAN

Table 2-2 lists the release history for this feature. Only features that were introduced or modified in Release 4.2(1)SV1(5.1) or a later release appear in the table.

Table 2-2 Feature History for VXLAN

Feature Name	Releases	Feature Information
VXLAN	4.2(1)SV1(5.1)	Introduced the Virtual Extensible Local Area Network (VXLAN) feature.

Send document comments to nexus1k-docfeedback@cisco.com.

INDEX

Send document comments to nexus1k-docfeedback@cisco.com.