



## CHAPTER 2

# Configuring Network Segmentation Manager

---

This chapter describes how to configure the Network Segmentation Manager and includes the following sections:

- [Prerequisites, page 2-1](#)
- [Guidelines and Limitations, page 2-2](#)
- [Default Settings, page 2-2](#)
- [Network Segmentation Manager Configuration Process, page 2-3](#)
- [Verifying the NSM Configuration, page 2-11](#)
- [Configuration Examples for Network Segmentation Manager, page 2-12](#)
- [Changing a Port Profile Associated with a Network Segmentation Policy, page 2-13](#)
- [Changing the Network Segmentation Policy Associated with a Network., page 2-16](#)
- [Feature History for Network Segmentation Manager, page 2-19](#)

## Information About Network Segmentation Manager

For more information, see the [Information About Network Segmentation Manager, page 1-3](#).

## Prerequisites

Network Segmentation Manager has the following prerequisites:

- You have installed the Cisco Nexus 1000V software and configured the following using the *Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(5.1)*.
- You have a vCenter Server 4.1 or 5.0 configured in vCloud Director 1.5 and vShield Manager 5.
- You have associated a vShield Manager with every vCenter Server.
- You have created an organization in vCloud Director.
- You have created provider and organization vDC in vCloud Director.
- Ensure that Virtual Supervisor Module (VSM) has an active SVS connection.
- Ensure that Virtual Supervisor Module (VSM)- Virtual Ethernet Module (VEM) connectivity is functioning.
- You have added hosts to Cisco Nexus 1000V.

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

- Ensure that the user specified for NSM on vShield Manager is a network administrator.

## Guidelines and Limitations

Network Segmentation feature has the following configuration guidelines and limitations:

- You must enable the VLANs that are going to be used through NSM and add them to the uplink.
- Ensure that the infrastructure has port 443 open.
- You must enable feature http-server in order to allow web service communication.
- You must enable the segmentation feature in order to use NSM for Virtual Extensible Local Area Network (VXLAN) via vCloud Director. In a network segmentation policy, VXLAN is used for a segmentation policy. See the *Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)*.

## Default Settings

Table 2-1 lists the default settings for network segmentation policies.

**Table 2-1**      **Default Network Segmentation Policies**

Parameters	Default
VLAN policy (port-profile template)	default_vlan_template
segmentation policy (port-profile template)	default_segmentation_template



### Note

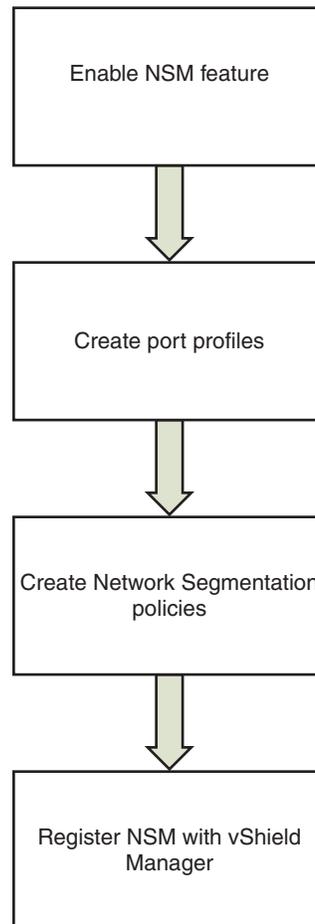
If a network creation request comes with a tenant ID and backing type that does not match a network segmentation policy, the default\_vlan\_template or default\_segmentation\_template is used during network creation from vCloud Director. In a network segmentation policy, VXLAN is used for a segmentation policy. For more information, see the *Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)*. If required, you can add additional policies to the default NSM template.

*Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).*

## Network Segmentation Manager Configuration Process

The following section guides you through the NSM configuration process. See [Figure 2-1](#). After completing each procedure, return to this section to make sure that you have completed all required procedures in the correct sequence.

**Figure 2-1** Network Segmentation Manager Configuration Process



331006

- 
- Step 1** Enable the NSM feature using the [“Enabling the NSM Feature”](#) section on page 2-3.
  - Step 2** Create a port profile for network segmentation policies using the [“Creating a Port Profile for Network Segmentation Policies”](#) section on page 2-5.
  - Step 3** Create network segmentation policies using the [“Creating Network Segmentation Policies”](#) section on page 2-6.
  - Step 4** Register NSM with vShield Manager using the [“Registering vShield Manager with Network Segmentation Manager”](#) section on page 2-10.

### Enabling the NSM Feature

You can enable the NSM feature in Cisco Nexus 1000V.

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

## SUMMARY STEPS

- configure terminal
- feature network-segmentation-manager
- (Optional) show network-segment manager switch

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> n1000v# <b>configure terminal</b> n1000v(config)#	Enters global configuration mode.
Step 2	<b>feature network-segmentation-manager</b>  <b>Example:</b> n1000v(config)# <b>feature network-segmentation-manager</b> n1000v(config)#	Enables the Network Segmentation Manager feature.
Step 3	<b>show network-segment manager switch</b>  <b>Example:</b> n1000v# <b>show network-segment manager switch</b> switch: default_switch state: enabled dvs-uuid: d4 e7 12 50 89 db 3b c4-8d 4d 4c 36 ca 1c d1 f0 dvs-name: nexus1000v mgmt-srv-uuid: 087F202C-8937-4F1E-8676-6F714C1AB96C reg status: unregistered last alert: - seconds ago connection status: disconnected	(Optional) Displays the Cisco Nexus 1000V configured with NSM.

## EXAMPLES

This example shows how to enable the NSM feature:

```
n1000v# configure terminal
n1000v(config)# feature network-segmentation-manager
n1000v# show network-segment manager switch
switch: default_switch
state: enabled
dvs-uuid: d4 e7 12 50 89 db 3b c4-8d 4d 4c 36 ca 1c d1 f0
dvs-name: nexus1000v
mgmt-srv-uuid: 087F202C-8937-4F1E-8676-6F714C1AB96C
reg status: unregistered
last alert: - seconds ago
connection status: disconnected
```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## Creating a Port Profile for Network Segmentation Policies

You can create a port profile that contains policies such as QoS, ACLs, and so on for network segmentation policies in Cisco Nexus 1000V.

For more information on port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SVI(5.1)*.

For more information on QoS, see the *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SVI(5.1)*.

For more information on ACL, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SVI(5.1)*.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- The VSM is connected to vCenter Server.
- The NSM feature is enabled.

### SUMMARY STEPS

1. **configure terminal**
2. **port-profile** [type vethernet] *name*
3. **no shutdown**
4. **state enabled**
5. **(Optional) show running-config port-profile** *name*

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> n1000v# <b>configure terminal</b> n1000v(config)#	Enters global configuration mode.
Step 2	<b>port-profile [type vethernet] name</b> <b>Example:</b> n1000v(config)# <b>port-profile type vethernet ABC_profile_segmentation</b> n1000v(config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 3	<b>no shutdown</b> <b>Example:</b> n1000v(config-port-prof)# <b>no shutdown</b> n1000v(config-port-prof)#	Administratively enables all ports in the profile.
Step 4	<b>state enabled</b> <b>Example:</b> n1000v(config-port-prof)# <b>state enabled</b> n1000v(config-port-prof)#	Enables the port profile and applies its configuration to the assigned ports.
Step 5	<b>show running-config port-profile</b> <b>Example:</b> n1000v(config-port-prof)# <b>show running-config port-profile ABC_profile_segmentation</b>	(Optional) Displays the configuration for verification.

## EXAMPLES

This example shows how to create a segmentation type port profile:

```
n1000v# configure terminal
n1000v(config)# port-profile type vethernet ABC_profile_segmentation
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)# state enabled
n1000v(config-port-prof)# show running-config port-profile ABC_profile_segmentation
!Command: show running-config port-profile ABC_profile_segmentation
!Time: Thu Dec 1 19:58:44 2011

version 4.2(1)SV1(5.1)
port-profile type vethernet ABC_profile_segmentation
  no shutdown
  state enabled
```

## Creating Network Segmentation Policies

Network segmentation policies are a set of policies that are inherited on a port profile that is created as a result of a network. The policy type can be either VLAN or Segmentation. This policy type corresponds to the network pool type in the vCloud Director. VLAN network segmentation policies are used for networks created from VLAN-backed network pools and Segmentation network segmentation policies are used for networks created from network isolation-backed network pools.

The network segmentation policies also contains a tenant ID and a reference to a port profile that may contain other policies for features such as QoS, ACL, and so on. Each tenant ID is unique and can be associated with only one Segmentation and one VLAN network segmentation policy. The tenant ID

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

correlates to the Organization Universally Unique Identifier (UUID) in the vCloud Director. For more information on retrieving the organization UUID from VMware vCloud Director, see [http://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=2012943](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2012943)

**Note**

If a network segmentation policy with a tenant ID is not created, the `default_vlan_template` or `default_segmentation_template` is used during network creation from vCloud Director. In a network segmentation policy, VXLAN is used for a segmentation policy. For more information, see the *Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)*.

You can create network segmentation policies.

**BEFORE YOU BEGIN**

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- The NSM feature is enabled.
- You know the tenant IDs for tenants that require non default network segmentation policies. The tenant IDs for network segment policies can be found on vCloud Director. It is located in the address bar of the browser when viewing an organization.

In the following example,

```
https://[VCloud_director_IP]/cloud/#/vAppListPage?org=91e87e80-e18b-460f-a761-b978c0d28aea
```

the tenant ID is "91e87e80-e18b-460f-a761-b978c0d28aea"

- You must create the port profiles with all the required feature port profiles before importing them to the network segmentation policy. To create a port profile, see the “[Creating a Port Profile for Network Segmentation Policies](#)” section.
- You have knowledge about port profile inheritance. See the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*.

**SUMMARY STEPS**

1. **configure terminal**
2. **network-segment policy** *name*
3. **description** *description*
4. **type** {segmentation | VLAN}
5. **id** {vCloud Director Organization tenant-id}
6. **import port-profile** *name*
7. (Optional) **show running-config network-segment policy**

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>configure terminal Example: n1000v# configure terminal n1000v(config)#</pre>	Enters global configuration mode.
Step 2	<pre>network-segment policy name Example: n1000v(config)# network-segment policy abc-policy-vxlan n1000v(config-network-segment-policy)#</pre>	Creates a network segmentation policy. The policy name can be up to 80 characters and must be unique for each policy on the NSM.
Step 3	<pre>description description Example: n1000v(config-network-segment-policy)# description network segmentation policy for ABC n1000v(config-network-segment-policy)#</pre>	Adds a description of up to 80 ASCII characters to the policy.
Step 4	<pre>type {segmentation   VLAN} Example: n1000v(config-network-segment-policy)# type segmentation n1000v(config-network-segment-policy)#</pre>	<p>Defines the network segmentation policy type. The policy type can be Segmentation or VLAN. For segmentation policy, VXLAN is used. For more information, see the <i>Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV1(5.1)</i>.</p> <p>The policy type corresponds to the network pools (VLAN-backed or network isolation-backed) in the vCloud Director.</p> <p>Once configured, the type cannot be changed.</p>
Step 5	<pre>id {vCloud Director Organization tenant-id} Example: n1000v(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170 n1000v(config-network-segment-policy)#</pre>	Associates the network segmentation policy with the tenant ID. The tenant ID correlates to the Organization UUID in the vCloud Director and cannot be changed once it is configured.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

	Command	Purpose
Step 6	<pre>import port-profile name Example: n1000v(config-network-segment-policy)# import port-profile ABC_profile_segmentation n1000v(config-network-segment-policy)#</pre>	Associates the port profile with the network segmentation policy. Each network created that uses this network segmentation policy will inherit the associated port profile.
Step 7	<pre>show running-config network-segment policy Example: n1000v#show running-config network-segment policy abc-policy-vxlan  !Command: show running-config network-segment policy abc-policy-vxlan !Time: Fri Aug 26 18:34:50 2011  version 4.2(1)SV1(5.1) feature network-segmentation-manager  network-segment policy abc-policy-vxlan description network segmentation policy for ABC for VXLAN networks id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170 type segmentation import port-profile port-profile ABC_profile_segmentation</pre>	(Optional) Displays the network segmentation policy configuration.

## EXAMPLES

This example shows how to create a NSM policy for ABC Inc for VXLAN networks:

```
n1000v# configure terminal
n1000v(config)# network-segment policy abc-policy-vxlan
n1000v(config-network-segment-policy)# description network segmentation policy for ABC for
VXLAN networks
n1000v(config-network-segment-policy)# type segmentation
n1000v(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
n1000v(config-network-segment-policy)# import port-profile ABC_profile_segmentation
n1000v(config-network-segment-policy)#show running-config network-segment policy
abc-policy-vxlan
!Command: show running-config network-segment policy abc-policy-vxlan
!Time: Fri Aug 26 18:34:50 2011

version 4.2(1)SV1(5.1)
feature network-segmentation-manager

network-segment policy abc-policy-vxlan
description network segmentation policy for ABC for VXLAN networks
id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
type segmentation
import port-profile port-profile ABC_profile_segmentation
```

This example shows how to create a NSM policy for ABC Inc for VLAN networks:

```
n1000v# configure terminal
n1000v(config)# network-segment policy abc-policy-vlan
n1000v(config-network-segment-policy)# description network segmentation policy for ABC for
VLAN networks
n1000v(config-network-segment-policy)# type vlan
n1000v(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
n1000v(config-network-segment-policy)# import port-profile ABC_profile_vlan
```

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

```
n1000v(config-network-segment-policy)#
```



**Note**

As a best practice, if a tenant specific policy is defined through network segmentation policies, you should define it for both segmentation and VLAN types.

## Registering vShield Manager with Network Segmentation Manager

You can use this procedure to register VMware vShield Manager with NSM.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to vShield Manager.
- The vShield Manager is connected to vCenter Server.
- The NSM feature is enabled.
- You know the range of multicast addresses.
- You know the segment ID pool.
- Ensure that the segment ID range allocated to vShield Manager does not overlap with other instances in the network or VXLANs used on the Cisco Nexus 1000V.
- Ensure that the user specified for NSM on vShield Manager is a network administrator.

### DETAILED STEPS

- 
- Step 1** In the vShield Manager, navigate to the Settings and Report window.
- Step 2** In the Setting and Reports pane, click **Configuration**.
- Step 3** Click **Networking**. The Edit Settings window opens.
- Step 4** Enter the segment ID pool. The segment ID pool should be greater than 4097.
- Step 5** Enter the multicast address range.
- Step 6** Click **OK**.
- Step 7** In the vShield Manager, navigate to the External Switch Providers window.
- Step 8** Click **Add Switch Provider**. The External Switch Provider window opens.
- Step 9** Enter the name of the switch.
- Step 10** Enter the NSM API service URL (<https://Cisco-VSM-IP-Address/n1k/services/NSM>).
- Step 11** Enter the network administrator username and password.
- Step 12** Accept the SSL thumbprint.
- Step 13** In the External Switch Providers window, a green check mark in the Status column indicates that the connection between vShield Manager and NSM is established.
- Step 14** You can verify the registration of the vShield Manager with NSM by entering the following command on the Cisco Nexus 1000V CLI:

```
n1000v# show network-segment manager switch
switch: default_switch
state: enabled
```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

```
dvs-uuid: d4 e7 12 50 89 db 3b c4-8d 4d 4c 36 ca 1c d1 f0
dvs-name: nexus1000v
mgmt-srv-uuid: 087F202C-8937-4F1E-8676-6F714C1AB96C
reg status: registered
last alert: 30 seconds ago
connection status: connected
```

## Unregistering vShield Manager with Network Segmentation Manager

You can use this procedure to unregister VMware vShield Manager with NSM.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to vShield Manager.
- The vShield Manager is registered with NSM.

### DETAILED STEPS

- Step 1** In the vShield Manager, navigate to the Settings and Report window.
- Step 2** In the Setting and Reports pane, click **Configuration**.
- Step 3** Click **Networking**. The Edit Settings window opens.
- Step 4** In the External Switch Providers pane, click the **Delete** link for the switch you wish to unregister.
- Step 5** You can verify that the vShield Manager has been unregistered by entering the following command on the Cisco Nexus 1000V CLI:

```
n1000v# show network-segment manager switch
switch: default_switch
state: enabled
dvs-uuid: ff 05 32 50 5b d5 db fe-da 48 70 e1 0f bd ae 43
dvs-name: cinquedia-vsm
mgmt-srv-uuid: 35B101C8-DE9B-42F9-BE85-284DD679367D
reg status: unregistered
last alert: - seconds ago
connection status: disconnected
```

## Verifying the NSM Configuration

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

Command	Purpose
<code>show network-segment manager switch</code>	Displays the Cisco Nexus 1000V configured with NSM.
<code>show running-config port-profile</code>	Displays the port profile configuration.
<code>show running-config network-segment policy</code>	Displays the NSM policy configuration.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

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)*.

## Configuration Examples for Network Segmentation Manager

The following example shows how to configure Network Segmentation Manager feature:

### Step 1 Enable Network Segmentation Manager.

```
n1000v# configure terminal
n1000v(config)# feature network-segmentation-manager
```

### Step 2 Create a port profiles for segmentation and VLAN policies.

```
n1000v# configure terminal
n1000v(config)# port-profile type vethernet ABC_profile_segmentation
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)# state enabled
```

```
n1000v# configure terminal
n1000v(config)# port-profile type vethernet ABC_profile_vlan
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)# state enabled
```

### Step 3 Create a NSM Policy

```
n1000v# configure terminal
n1000v(config)# network-segment policy abc-policy-vxlan
n1000v(config-network-segment-policy)# description network segmentation policy for ABC for
VXLAN networks
n1000v(config-network-segment-policy)# type segmentation
n1000v(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
n1000v(config-network-segment-policy)# import port-profile ABC_profile_segmentation

n1000v#configure terminal
n1000v(config)# network-segment policy abc-policy-vlan
n1000v(config-network-segment-policy)# description network segmentation policy for ABC for
VLAN networks
n1000v(config-network-segment-policy)# type vlan
n1000v(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
n1000v(config-network-segment-policy)# import port-profile ABC_profile_vlan
```

### Step 4 Verify the configuration.

```
n1000v# configure terminal
n1000v(config)# show running-config network-segment policy abc-policy-vxlan
!Command: show running-config network-segment policy abc-policy-vxlan
!Time: Fri Aug 26 18:34:50 2011

version 4.2(1)SV1(5.1)
feature network-segmentation-manager

network-segment policy abc-policy-vxlan
description network segmentation policy for ABC for VXLAN networks
id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
type segmentation
import port-profile port-profile ABC_profile_segmentation
```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## Changing a Port Profile Associated with a Network Segmentation Policy

During a network creation in the vCloud Director, network segmentation policies are created on the NSM and these network segmentation policies are inherited on a port profile. In order to associate a different port profile with the deployed network, you can change the port profile associated with the network segmentation policy.

To change the port profile associated with the network segmentation policy perform the following steps:

- 
- Step 1** Identify all the networks associated with the network segmentation policy. For more information, see [Identifying the Networks Associated with the Network Segmentation Policy, page 2-13](#).
  - Step 2** Manually remove the inheritance for the existing port profile. See section “Removing Inherited Policies from a Port Profile” in the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)* for more information.
  - Step 3** Manually inherit the new port profile that will be associated with the network segmentation policy. See section “Inheriting a Configuration from a Port Profile” in the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)* for more information.
  - Step 4** Update the network segmentation policy. For more information, see [Updating the Network Segmentation Policy, page 2-14](#)
- 

## Identifying the Networks Associated with the Network Segmentation Policy

You can identify the networks associated with the network segmentation policy.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in configuration mode.
- The NSM feature is enabled.

### SUMMARY STEPS

1. **configure terminal**
2. **show network-segment policy usage**

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## DETAILED STEPS

	Command	Description
Step 1	<b>configure terminal</b>  <b>Example:</b> n1000v# configure terminal n1000v(config)#	Enters global configuration mode.
Step 2	<b>show network-segment policy usage</b> <b>Example:</b> n1000v(config)# <b>show network-segment policy usage</b>	Displays the network segmentation policy usage by networks.

## EXAMPLES

This example shows how to identify the networks associated with a network segmentation policy:

```
n1000v(config)# show network-segment policy usage

network-segment policy default_segmentation_template
dvs.VCDVSint-org-cn2-e46e9686-2327-49df-ad5c-a3f89c00cfb8

network-segment policy default_vlan_template

network-segment policy abc-policy-vxlan
dvs.VCDVSint-org-nexus-6141babd-bdc8-4e86-8f16-1ac786fb377f

network-segment policy abc-policy-vlan
```

## Updating the Network Segmentation Policy

You can update a network segmentation policy.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- The NSM feature is enabled.
- You know the tenant IDs for tenants that require non default network segmentation policies.
- You must create the port profiles with all the required feature port profiles before importing them to the network segmentation policy. To create a port profile, see the [Creating a Port Profile for Network Segmentation Policies, page 2-5](#).
- You have knowledge about port profile inheritance. See the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*.

### SUMMARY STEPS

1. **configure terminal**
2. **network-segment policy** *name*
3. **import port-profile** *name force*

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

#### 4. (Optional) show run network-segment policy

### DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> n1000v# <b>configure terminal</b> n1000v(config)#	Enters global configuration mode.
Step 2	<b>network-segment policy name</b> <b>Example:</b> n1000v(config)# <b>network-segment policy abc-policy-vxlan</b> n1000v(config-network-segment-policy)	Creates a network segmentation policy. The policy name can be up to 80 characters and must be unique for each policy on the NSM.
Step 3	<b>import port-profile name force</b> <b>Example:</b> n1000v(config-network-segment-policy) # <b>import port-profile ABC_profile_segmentation force</b> n1000v(config-network-segment-policy)	Forces the new port profile to be used and migrates existing the networks to the new port profile. Each network created that uses this network segmentation policy will inherit the associated port profile.  <b>Note</b> The force option overrides any checks in the NSM that prevent you from modifying the port profile. After updating the network segmentation policy, a warning is displayed listing any networks that are not inheriting the new port profile.
Step 4	<b>show running-config network-segment policy</b> <b>Example:</b> n1000v(config-network-segment-policy) # <b>show running-config network-segment policy abc-policy-vxlan</b>	(Optional) Displays the network segmentation policy configuration.

### EXAMPLES

This example shows how to update the network segmentation policy:

```
n1000v# configure terminal
n1000v(config)# show running-config network-segment policy abc-policy-vxlan

network-segment policy abc-policy-vxlan
description network segmentation policy for ABC for VXLAN networks
type segmentation
id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
import port-profile ABC_profile_segmentation

n1000v(config)# network-segment policy abc-policy-vxlan
n1000v(config-network-segment-policy) # import port-profile ABC_profile_segmentation_new
force
n1000v(config)# show running-config network-segment policy abc-policy-vxlan

network-segment policy abc-policy-vxlan
description network segmentation policy for ABC for VXLAN networks
type segmentation
id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
import port-profile ABC_profile_segmentation_new
```

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

## Changing the Network Segmentation Policy Associated with a Network.

During a network creation in the vCloud Director, network segmentation policies are created on the NSM. In order to use other non default policies for any new or old networks associated with an Organization vDC in the vCloud Director, you must change the network segmentation policy associated with a network.

To change the network segmentation policy associated with a network, perform the following steps:

- 
- Step 1** Identify all the networks that need to be migrated. For more information, see [Identifying the Networks, page 2-16](#).
  - Step 2** Manually remove the inheritance of the port profile associated with the network segmentation policy from the network. See section “Removing Inherited Policies from a Port Profile” in the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)* for more information.
  - Step 3** Manually inherit the new port profile that will be associated with the network segmentation policy on the network. See section “Inheriting a Configuration from a Port Profile” in the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)* for more information.
  - Step 4** Migrate the networks from the default network segmentation policy to the non default network segmentation policy. For more information, see [Migrating Networks to Non Default Network Segmentation Policy, page 2-17](#).
- 

## Identifying the Networks

You can identify the networks that have to be migrated.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in configuration mode.
- The NSM feature is enabled.

### SUMMARY STEPS

1. **configure terminal**
2. **show network-segment network**

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## DETAILED STEPS

	Command	Description
Step 1	<code>configure terminal</code>  <b>Example:</b> n1000v# <code>configure terminal</code> n1000v(config)#	Enters global configuration mode.
Step 2	<code>show network-segment network</code> <b>Example:</b> n1000v(config)# <code>show network-segment network</code>	Displays the networks associated with a network segmentation policy.

## EXAMPLES

This example shows you how to display the networks associated with a network segmentation policy:

```
n1000v(config)# show network-segment network

network dvs.VCDVSint-org-cn2-e46e9686-2327-49df-ad5c-a3f89c00cfb8
tenant id: 2b4calb2-ba8e-456c-b772-a4730af16e2e
network-segment policy: default_segmentation_template
segment id: 4107
multicast ip: 225.0.0.1

network dvs.VCDVSint-org-nexus-6141babd-bdc8-4e86-8f16-1ac786fb377f
tenant id: 91e87e80-e18b-460f-a761-b978c0d28aea
network-segment policy: seg-template-nexus-org
segment id: 4108
multicast ip: 225.0.0.2

n1000v(config)#
```

## Migrating Networks to Non Default Network Segmentation Policy

You can migrate the networks from the default network segmentation policy to the non default network segmentation policy.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- The NSM feature is enabled.
- You know the tenant IDs for tenants that require non default network segmentation policies.
- You have knowledge about port profile inheritance. See the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*.

### SUMMARY STEPS

1. `configure terminal`
2. `network-segment policy migrate id isolation_id type nw_type dest-policy policy`
3. (Optional) `show network-segment network`

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>configure terminal Example: n1000v# config terminal n1000v(config)#</pre>	Enters global configuration mode.
Step 2	<pre>network-segment policy migrate id isolation_id type nw_type dest-policy policy Example: n1000v(config)# network-segment policy migrate id da5c49a8-dd1b-4326-9da0-3c5e6a2c1b87 type vlan dest-policy org_vlan</pre>	<p>Migrates the the networks from the default network segmentation policy to the non default destination network segmentation policy.</p> <ul style="list-style-type: none"> <li><i>isolation_id</i>: Tenant ID of for the networks to be migrated.</li> <li><i>nw_type</i>: Type of networks (VLAN or Segmentation) to be migrated</li> <li><i>policy</i>: Name of the destination network segmentation policy to migrate to.</li> </ul> <p><b>Note</b> If there are any existing networks that match the tenant ID and type, but are not inheriting the port profile associated with the destination network segmentation policy, a warning will be displayed listing the port-profiles that are not migrated.</p>
Step 3	<pre>show network-segment network</pre>	(Optional) Displays the networks associated with a network segmentation policy.

## EXAMPLES

This example shows you how to migrate networks to non default segmentation policy:

```
n1000v(config)# show network-segment network
```

```
network dvs.VCDVStenantid_vlan-74e36255-e588-4357-8abe-15d2cc7feaec
tenant id: da5c49a8-dd1b-4326-9da0-3c5e6a2c1b87
network-segment policy: default_segmentation_template
segment id: 4107
multicast ip: 225.0.0.1
```

```
n1000v(config)# network-segment policy migrate id da5c49a8-dd1b-4326-9da0-3c5e6a2c1b87
type segmentation dest-policy org_seg
```



### Note

In case a warning appears then, first manually remove the inheritance of the port profile associated with the network segmentation policy from the network. See section “Removing Inherited Policies from a Port Profile” in the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)* for more information. Then, manually inherit the new port profile that will be associated with the network segmentation policy on the network. See section “Inheriting a Configuration from a Port Profile” in the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)* for more information.

```
n1000v(config)#show network-segment network
```

```
network dvs.VCDVStenantid_vlan-74e36255-e588-4357-8abe-15d2cc7feaec
tenant id: da5c49a8-dd1b-4326-9da0-3c5e6a2c1b87
```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

```
network-segment policy: org_seg
segment id: 4107
multicast ip: 225.0.0.1
```

## Feature History for Network Segmentation Manager

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 NSM***

Feature Name	Releases	Feature Information
Network Segmentation Manager	4.2(1)SV1(5.1)	Introduced the Network Segmentation Manager (NSM) feature.

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***