CHAPTER 1

Overview

This chapter provides an overview of the Cisco Nexus 1000V port profiles and includes the following sections:

Understanding Port Profiles

In Cisco Nexus 1000V, port profiles are used to configure interfaces. A port profile can be assigned to multiple interfaces giving them all the same configuration. Changes to the port profile can be propagated automatically to the configuration of any interface assigned to it.

In the VMware vCenter Server, a port profile is represented as a port group. The VEthernet or Ethernet interfaces are assigned in vCenter Server to a port profile for:

- Defining port configuration by policy.
- Applying a single policy across a large number of ports.
- Supporting both VEthernet and Ethernet ports.

Port profiles that are configured as uplinks, can be assigned by the server administrator to physical ports (a vmnic or a pnic). Port profiles that are not configured as uplinks can be assigned to a VM virtual port.

Note While manual interface configuration overrides that of the port profile, it is not recommended. Manual interface configuration is only used, for example, to quickly test a change or allow a port to be disabled without having to change the inherited port profile.

For more information about assigning port profiles, see your VMware documentation.

To verify that the profiles are assigned as expected, use the following show commands:

show port-profile usage

show running-config interface *interface-id*

Note: The output of the command **show running-config interface** *interface-id* shows a config line such as, `inherit port-profile MyProfile,` indicating the inherited port profile.

Note Inherited port profiles cannot be changed or removed from an interface using the Cisco Nexus 1000V CLI. This can only be done through the vCenter Server.

Note Inherited port profiles are automatically configured by the Cisco Nexus 1000V when the ports are attached on the hosts. This is done by matching up the VMware port group assigned by the system administrator with the port profile that created it.

Port Profile States

Port profiles are disabled by default. The following table describes port profile behavior in the two states. To enable a port profile, see the "Enabling a Port Profile" procedure on page 1-33.

State	Behavior
Disabled (the default)	When disabled, a port profile behaves as follows: • Its configuration is not applied to assigned ports. • If exporting policies to a VMware port group, the port group is not created on the vCenter Server.
Enabled	When enabled, a port profile behaves as follows: • Its configuration is applied to assigned ports. • If inheriting policies from a VMware port group, the port group is created on the vCenter Server.

Port Profile Characteristics

The following characteristics can be configured for a port profile. For detailed port profile configuration procedures, see the section, Port Profile Configuration, page 1-1.

Table 1-1 Port Profile Characteristics

Port Profile Characteristics
acl
capability (uplink, l3control)
channel-group
default (resets characteristic to its default)
description
inherit
interface state (shut/no shut)
name
netflow

Table 1-1 Port Profile Characteristics (continued)

Port Profile Characteristics
port security
private vlan configuration
qos policy
state (enabled or disabled)
switchport mode (access or trunk)
system vlan *vlan list*
vlan configuration
vmware max-ports
vmware port-group name

Port Profile Inheritance

One port profile can be configured to inherit the policies from another port profile. The characteristics of the parent profile become the default settings for the child. The inheriting port profile ignores any non-applicable configuration.

The following table shows port profile characteristics and whether they can be inherited.

Table 1-2 Port Profile Inheritance

	Can it be inherited?	
Port Profile Characteristic	**Yes**	**No**
acl	X	
capability (uplink, l3control)		X
channel group	X	
default (resets characteristic to its default)	X	
description		X
inherit	X	
interface state (shut/no shut)	X	
name	X	
netflow	X	
port security	X	
private vlan configuration	X	
qos policy	X	
state (enabled or disabled)		X
switchport mode (access or trunk)	X	
system vlan *vlan list*		X
vlan configuration	X	

Table 1-2 Port Profile Inheritance (continued)

Port Profile Characteristic	Can it be inherited?	
	Yes	No
acl	X	
capability (uplink, l3control)		X
channel group	X	
vmware max-ports		X
vmware port-group name		X

Using the CLI , you can configure alternate characteristics directly on the new port profile to override the inherited characteristics.

You can also explicitly remove port profile inheritance, so that a port profile returns to normal defaults except where there has been direct configuration.

For more information, see the procedure, Inheriting a Port Profile Configuration, page 1-9.

Information about the System Port Profile

A system port profile is designed to establish and protect vCenter Server connectivity. They can carry the following VLANs:

- System VLANs or VNICs used when bringing up the ports before communication is established between the VSM and VEM.
- The uplink that carries the control VLAN
- Management uplink(s) used for VMWare vCenter Server connectivity or SSH or Telnet connections. There can be more than one management port or VLAN, for example, one dedicated for vCenter Server connectivity, one for SSH, one for SNMP, a switch interface, and so forth.
- VMware kernel NIC for accessing VMFS storage over iSCSI or NFS.

System Port Profile Rules

System port profiles and system VLANs are subject to the following rules.

- System VLANs cannot be deleted when the profile is in use.
- Non-system VLANs in a system port profile can be freely added or deleted, even when the profile is in use, that is, one or more DVS ports are carrying that profile.
- System VLANs can always be added to a system port profile or a non-system port profile, even when the profile is in use.
- The native VLAN on a system port profile may be a system VLAN or a non-system VLAN.

Use the following steps to change the set of system VLANs on a port profile without removing all system VLANs:

1. Remove all ports carrying the profile from the DVS.
2. Set the new list of system VLANs on the profile with the “system vlan …” command. The new list may add or delete system VLANs from the old list.
3. Add the the ports back to the DVS with the same profile.

Use the following steps to remove all system VLANs from a port:

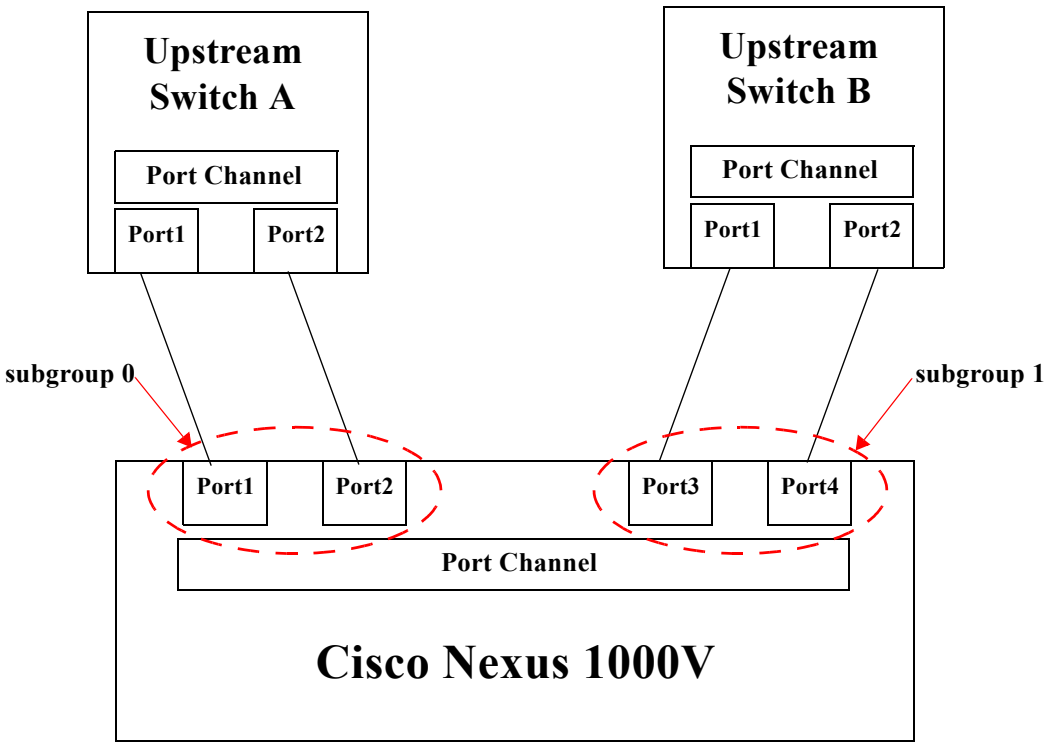
1. Remove all ports carrying the port profile from the DVS, if you plan to modify the system profile.
2. Prepare a port profile without system VLANs, either by modifying the old port profile or by creating a new one.
3. Reboot the VEM host where the port resides.
4. Apply the non-system profile to the port.

vPC Host Mode

Virtual port channel host mode (vPC-HM) allows member ports in a port channel to connect to two different upstream switches. With vPC-HM, ports are grouped into two subgroups for traffic separation. If CDP is enabled on the upstream switch, then the subgroups are automatically created using CDP information. If CDP is not enabled on the upstream switch, then you must manually create the subgroup on the interface.

As shown in Figure 1-1, in vPC-HM, member ports are assigned a subgroup ID (0 or 1)for traffic separation.

Figure 1-1 Using vPC-HM to Connect a Port Channel to Two Separate Upstream Switches



To configure a port profile in vPC-HM, see the "Configuring a Port Channel Connecting to Two Upstream Switches" procedure on page 1-20.

vPC-HM can also be configured on the interface. For more information, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(1)*.