Migration from VMware vSwitch to Cisco Nexus 1000V

Introduction

Cisco Nexus 1000V Series Switches are virtual machine access switches that are an intelligent software switch implementation for VMware vSphere environments running the Cisco NX-OS Software operating system. Operating inside the VMware ESX hypervisor, the Cisco Nexus 1000V Series supports Cisco VN-Link server virtualization technology to provide:

- Policy-based virtual machine connectivity
- Mobile virtual machine security and network policy
- Nondisruptive operational model for your server virtualization, and networking teams

When server virtualization is deployed in the data center, virtual servers typically are not managed the same way as physical servers. Server virtualization is treated as a special deployment, leading to longer deployment time, with a greater degree of coordination among server, network, storage, and security administrators. With the Cisco Nexus 1000V Series, you can have a consistent networking feature set and provisioning process all the way from the virtual machine access layer to the core of the data center network infrastructure. Virtual servers can now use the same network configuration, security policy, diagnostic tools, and operational models as their physical server counterparts attached to dedicated physical network ports. Virtualization administrators can access predefined network policy that follows mobile virtual machines to help ensure proper connectivity, saving valuable time to focus on virtual machine administration. This comprehensive set of capabilities helps you deploy server virtualization faster and gain its benefits sooner.

Developed in close collaboration with VMware, the Cisco Nexus 1000V Series is certified by VMware to be compatible with VMware vSphere, vCenter, ESX, and ESXi, and with many other VMware vSphere features. You can use the Cisco Nexus 1000V Series to manage your virtual machine connectivity with confidence in the integrity of the server virtualization infrastructure.

Overview:

This document provides guidance for migrating from the VMware vSwitch to the Cisco Nexus™ 1000V Series Switches. It will cover the necessary steps for each of the following migration options:

1. Considerations for migrating multiple VMware vSwitches to a single Cisco Nexus 1000V Virtual Ethernet Module
2. Migrating physical hosts from the VMware vSwitch to the Cisco Nexus 1000 distributed virtual switch
3. Migrating VMware port-groups to Cisco Nexus 1000V port-profiles
4. Migrating Virtual Machines from the vSwitch to the Nexus 1000V
5. Migration using VMware host profiles

For detailed configuration documentation, please refer to the respective Cisco® and VMware product configuration guides.

Audience:

This document is intended for network architects, network engineers, virtualization administrators, and server administrators interested in understanding and deploying VMware vSphere 4.0 hosts in a Cisco data center environment. It is assumed that the user is familiar with the Cisco Nexus 1000V components and configuration.

Prerequisites:

It is assumed the user is familiar with Cisco Nexus 1000V , Cisco's NX-OS Operating System and VMware vSphere4. It is also assumed that the user has or will be able to achieve the following:

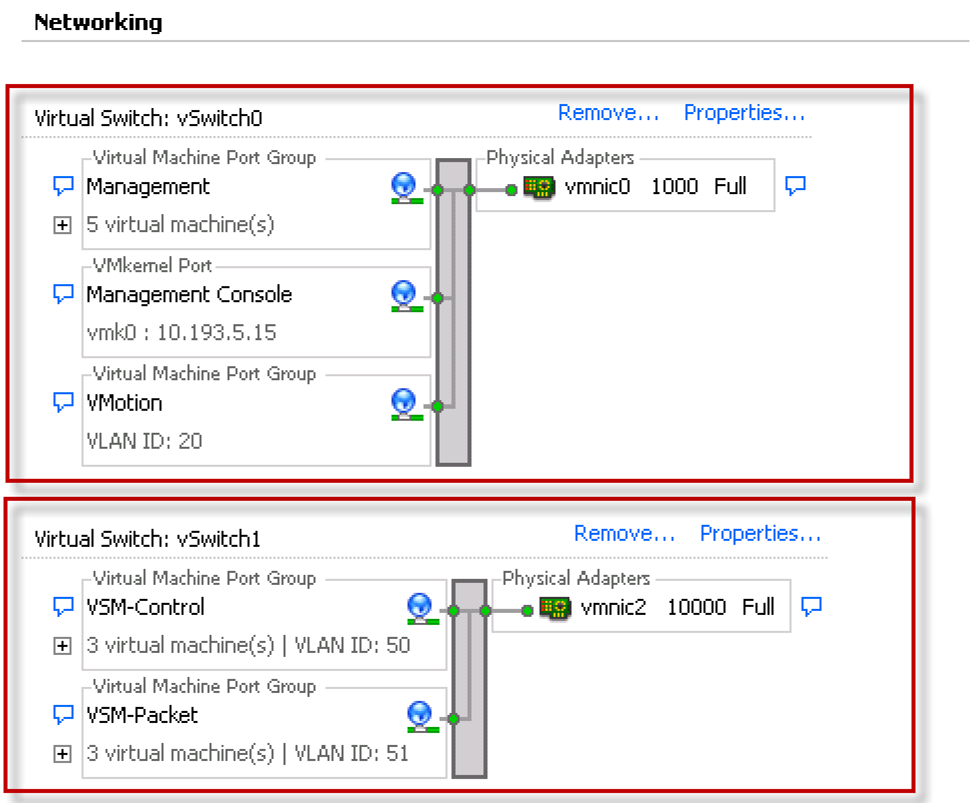
- Successfully install the Cisco Nexus 1000V VSM as described in the *Software Install Guide – "Installing and Configuring the VSM VM"*.
- The VSM VM has network connectivity as described in *Software Install Guide – "Verifying VSM Connectivity"*
- Able to successfully connect to the vCenter server as described in the Software Install Guide – "Connecting to the vCenter Server"
- Successfully install the VEM software on the ESX host as described in the *VEM Install Guide*

Considerations for Migrating Multiple vSwitches to a Single VEM

In order to successfully migrate from the VMware vSwitch to the Cisco Nexus 1000V and benefit from the added advantages of a Cisco Switch, there are some minor differences between the Nexus 1000V and the vSwitch that the user should take into account.

The vSwitch, until now, has been used to bring network connectivity to the Virtual Machine. However the main challenges customers are facing when migrating to server virtualization is the lack of transparency of the individual Virtual Machine traffic and the change in operational model where the server admin is now responsible for that the network configuration including managing VLANs, NIC Teaming and Quality of Service parameters.

A VLAN is a well-known, fundamental configuration of the network that is often used to provide reliability, security and traffic separation throughout the network. Depending on the requirement or mindset of the server administrator team, there are instances where multiple vSwitches were used over VLANs to provide segregation of different traffic types and add another level of perceived security.


Networking

Virtual Switch: vSwitch0
Virtual Machine Port Group
Management
5 virtual machine(s)
VMkernel Port
Management Console
vmk0 : 10.193.5.15
Virtual Machine Port Group
VMotion
VLAN ID: 20
Physical Adapters
vmnic0 1000 Full

Virtual Switch: vSwitch1
Virtual Machine Port Group
VSM-Control
3 virtual machine(s) | VLAN ID: 50
Virtual Machine Port Group
VSM-Packet
3 virtual machine(s) | VLAN ID: 51
Physical Adapters
vmnic2 10000 Full

Figure 1 - Multiple VMware vSwitch Configuration Example

This argument is partially true from a configuration standpoint since it is not possible within VCenter to allow interfaces on the same vSwitch to contain different VLAN configurations. However the Cisco Nexus 1000V is configured and operated like any other Cisco Data Center switch and therefore meets all of the security requirements regarding the configuration, management and protection of a VLAN that customer deploy today. This means that the environments where multiple vSwitches are utilized can be duplicated with a single instance of the Virtual Ethernet Module (VEM) component of the Cisco Nexus 1000V. By moving from multiple vSwitches to an environment with a single VEM living on a host, management becomes simpler and the burden of creating different sets of VMware port-groups per vSwitch is eliminated.

The example shown in Figure 1 shows an environment where the server team has deployed two different vSwitches -- vSwitch0 and vSwitch1 – each configured to carry different VLANs. This configuration shows that on vSwitch0, vmnic0 is configured to allow VLAN 20 used by the port-group “VMotion” as well as the native VLAN used by the port-groups “Management Console” and “Management”. On vSwitch 1, vmnic2 is configured to carry both VLAN 50 and VLAN 51 for the perspective port-groups only.

With the Nexus 1000V the network administrator has the granularity of selecting which VLAN are allowed per uplink (vmnic port). And, like any other Cisco Data Center switch, the configuration will provide the associated security and protection of the traffic that the network team is used to.

The same configuration shown in Figure 1 can be achieved using the Nexus 1000V by configuring the uplink port-profile as follows:

vSwitch0 can be replaced with the port-profile configuration:

```
Pod2-Nexus1000V(config)# port-profile type ethernet system-uplink
Pod2-Nexus1000V(config-port-prof)# switchport mode trunk
Pod2-Nexus1000V(config-port-prof)# switchport trunk allowed vlan 1,20,21
Pod2-Nexus1000V(config-port-prof)# no shutdown
Pod2-Nexus1000V(config-port-prof)# system vlan 1,20-21
Pod2-Nexus1000V(config-port-prof)# state enabled
Pod2-Nexus1000V(config-port-prof)# vmware port-group
```

The network team is already well versed with the Cisco CLI so the VLAN configuration will be seamless. The above commands allow only the native vlan (shown here as vlan 1) and vlan 20 to use that physical link and therefore provides the same security and segregation of the traffic achieved by having vSwitch0.

vSwitch1 can be replaced with the port-profile configuration:

```
Pod2-Nexus1000V(config)# port-profile type ethernet vm-uplink
Pod2-Nexus1000V(config-port-prof)# switchport mode trunk
Pod2-Nexus1000V(config-port-prof)# switchport trunk allowed vlan 50-51
Pod2-Nexus1000V(config-port-prof)# no shutdown
Pod2-Nexus1000V(config-port-prof)# state enabled
Pod2-Nexus1000V(config-port-prof)# vmware port-group
```

This configuration will only allow vlan 50 and 51 on this link and therefore provides the same benefits as vSwitch1.

This simple configuration shows how the Cisco Nexus 1000V provides the same level of security and traffic separation found in other Cisco platforms through granular VLAN configuration and the ability to configure different VLAN policies per interface. This granularity of configuration will enable the network team to reproduce any vSwitch configuration without having the necessity of deploying multiple vSwitches and the port-group configuration burden that accompanies a multiple vSwitch deployment.

Migrating VMware Port-Groups to Cisco Nexus 1000V Port-Profiles

The Port Group is a concept brought by VMware that provides a configuration template that can be applied multiple times to different Virtual Machine. All of the virtual machines sharing the same port-group will also share the same network configuration including both VLAN and high availability configurations. Server Administrators use port-groups and apply them to virtual machines in order to configure their network parameters.

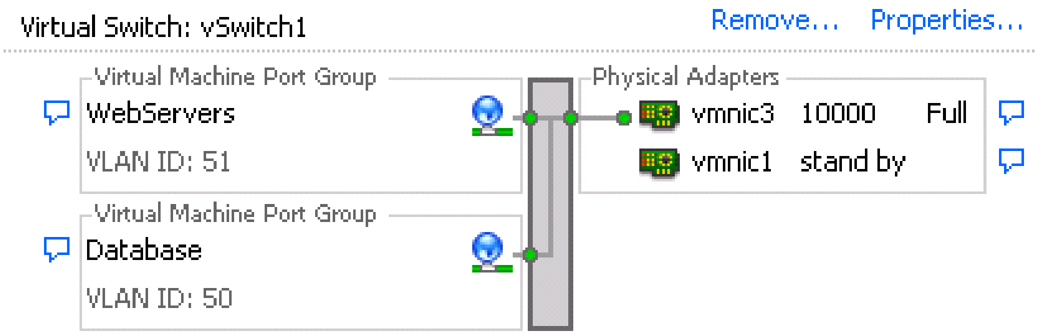
A port-group contains two very important network parameters: the vlan configuration and the NIC teaming configuration. NIC teaming is used by the vSwitch as a fail over mechanism and provide network redundancy for the virtual machines. This sections will focus on how to migrate both the vlan configuration and NIC teaming options used by the vSwitch to the Nexus 1000V.

The port-profile concept within the Cisco Nexus 1000V follows the same parameters but is used by the network to configure the actual network policies. Once a port-profile is configured on the Cisco Nexus 1000V by the Network Administrator, it translated into a VMware port-group and sent to VMware vCenter Server where the server administrator can then apply it to various virtual machines. A port profile for the network administrator is the equivalent of a port group for the server administrator. This configuration and translation allows Network administrators to retain their operation model of configuring network policies for each host – even if these hosts are now virtual machines.

This section will look at the necessary steps which are need to migrate pre-existing VMware port-groups into port-profiles configured from the Cisco Nexus 1000V.

Migrate the VLAN

Before the Nexus 1000V, the configuration of the VLAN for a particular port-group was done by the server team. The network team would provide a trunk from the physical upstream switch but have no control over the VLAN configuration at the host level. Therefore the network team had no visibility into the virtual network. Instead, interactions between the Network and Server teams were necessary in order to deploy the correct VLAN trunks on the correct physical links.



Virtual Switch: vSwitch1

WebServers
VLAN ID: 51

Database
VLAN ID: 50

vmnic3 10000 Full
vmnic1 stand by

Figure 2 - VMware Configuration for VLANs and NIC Failover

The vSwitch configuration shown in Figure 2 contains two VMware port-group associations: WebServers and Database. If the network administrator wants to reproduce the same configurations as the port-groups above with the Nexus 1000V, the configuration would be as follows:

for the WebServers port-profile:

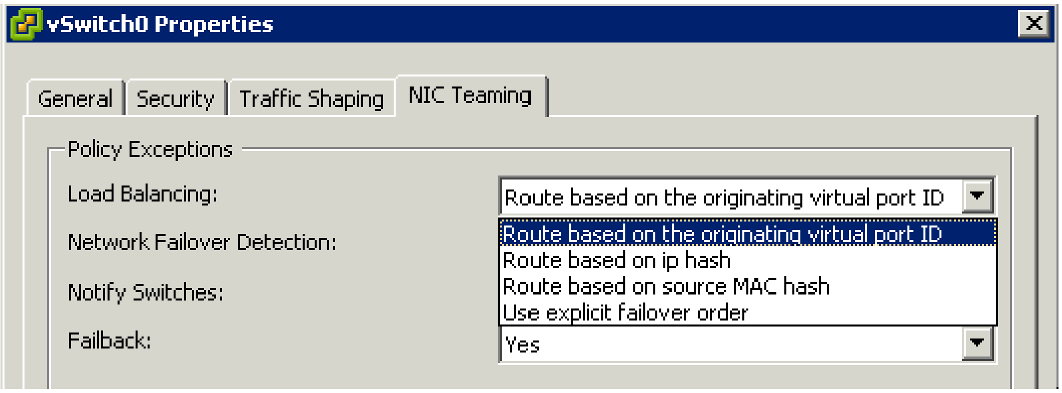
```
Pod2-Nexus1000V(config)# port-profile WebServers
Pod2-Nexus1000V(config-port-prof)# switchport mode access
Pod2-Nexus1000V(config-port-prof)# switchport access vlan 51
Pod2-Nexus1000V(config-port-prof)# no shut
```

for the Database port-profile:

```
Pod2-Nexus1000V(config)# port-profile Database
Pod2-Nexus1000V(config-port-prof)# switchport mode access
Pod2-Nexus1000V(config-port-prof)# switchport access vlan 50
Pod2-Nexus1000V(config-port-prof)# no shut
```

The above configuration not only recreates the existing VMware port-group configurations on the Cisco Nexus 1000V but it shows an example of how the network configuration will contain the same parameters and appear the same to network administrators weather the configuration is for a physical host or a virtual host. A virtual machine can now be handled the same way as a bare metal server. The virtual servers port configuration will continue to be configured as an access switchport, hence providing all the security associated to an access switchport in today's physical networks.

Migrate the vSwitch NIC Teaming



Load Balancing: Route based on the originating virtual port ID

Route based on the originating virtual port ID
Route based on ip hash
Route based on source MAC hash
Use explicit failover order

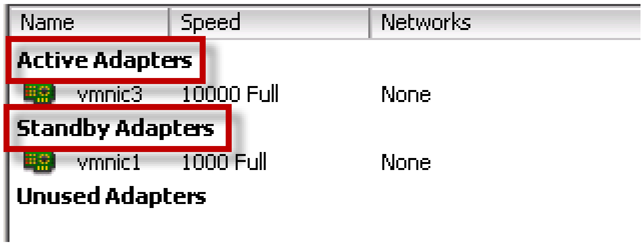
Network Failover Detection:

Notify Switches:

Failback: Yes

Figure 3 – Load-balancing options available on the VMware vSwitch

The VMware vSwitch contains 4 different options for load-balancing traffic across the physical NICs. These include hashing algorithms using virtual port IDs, IP addresses, MAC addresses and an option for explicit failover. VMware also offers the ability to choose which links are active and which are stand-by.



Name	Speed	Networks
Active Adapters		
vmnic3	10000 Full	None
Standby Adapters		
vmnic1	1000 Full	None
Unused Adapters		

Figure 4 – NIC Teaming options available on the VMware vSwitch

Load-balancing and teaming parameters will depend on the physical layout of the network. There are two options for connectivity: connecting the host to a single upstream switch and connecting the host to multiple upstream switches.

SINGLE SWITCH CONNECTIVITY

Connecting a host to a single upstream switch may be an unlikely deployment, however some users may chose this option when they need large amounts of bandwidth out of a host. VMware provides a load-balancing option based on IP hashing which means that flows coming from the same virtual machine can be load-balanced across the multiple uplinks out of the vSwitch. This requires that the upstream switch be configured as a port-channel with the channel-group mode turned “on”.

The Nexus 1000V improves on this deployment with the support for Link Aggregation Control Protocol (LACP). LACP not only makes the port channel configuration simpler and guard against configuration mismatches, but utilizing LACP between the Nexus 1000V and upstream switches means that the host can leverage the standard load-balancing algorithms offer by Cisco. There are currently 17 load-balancing algorithms offered including hashing based on Layer 2, Layer 3 and Layer 4 information.

A single command added to the Cisco Nexus 1000V uplink port-profile will enable this functionality:

```
Pod2-Nexus1000V(config)# port-profile type ethernet system-uplink
Pod2-Nexus1000V(config-port-prof)# switchport mode trunk
Pod2-Nexus1000V(config-port-prof)# switchport trunk allowed vlan 50-51
Pod2-Nexus1000V(config-port-prof)# channel-group auto mode active
```

The command **`channel-group auto mode active`** will automatically create a port-channel with the upstream switch using Link Aggregation Control Protocol (LACP).

MULTIPLE UPSTREAM SWITCH CONNECTIVITY

Connecting the host to multiple upstream switches offers redundancy for the host and is the typical deployment seen in the Data Center. Depending on the upstream switches, there are multiple design options for dual homing a single host.

The Cisco Nexus 1000V Design guide speaks to the different options available for multiple switch connectivity. If the upstream switches support a clustering technology such as VSS on the Catalyst 6500s or vPC on the Nexus 5000/7000 Series switches, it is recommended to leverage LACP on the

Nexus 1000V because of the benefits it offers in configuration, high availability and load-balancing options. If LACP is not available and the upstream switches do not support a clustering technology, then the recommendation is to deploy virtual port-channel host-mode (vPC-HM), using the mac-pinning option. vPC-HM is a configuration that is native to the Cisco Nexus 1000V switch. It allows for the creation of a port-channel interface even if the uplinks from the host are going to two different switches. To read more about the connection options when connecting to more than one upstream switch, please reference the Cisco Nexus 1000V Design Guide.

The configuration for using LACP between the Nexus 1000V and upstream switches includes the addition of the "**`channel-group auto mode active`**" command within the port-profile. The following configuration is an example of a complete uplink port-profile including the VLANs, LACP and system VLAN configurations.

```
Pod2-Nexus1000V(config)# port-profile type ethernet system-uplink
Pod2-Nexus1000V(config-port-prof)# vmware port-group
Pod2-Nexus1000V(config-port-prof)# switchport mode trunk
Pod2-Nexus1000V(config-port-prof)# switchport trunk allowed vlan 1,20-21,50-51
Pod2-Nexus1000V(config-port-prof)# channel-group auto mode active
Pod2-Nexus1000V(config-port-prof)# no shutdown
Pod2-Nexus1000V(config-port-prof)# system vlan 1,20,21
Pod2-Nexus1000V(config-port-prof)# state enable
```

The configuration for using vPC-HM with the mac-pinning option between the Nexus 1000V and upstream switches includes the addition of the "**`channel-group auto mode on mac-pinning`** " command within the port-profile. following configuration is an example of a complete uplink port-profile including the VLANs, vPC-HM and system VLAN configurations.

```
Pod2-Nexus1000V(config)# port-profile type ethernet system-uplink
Pod2-Nexus1000V(config-port-prof)# vmware port-group
Pod2-Nexus1000V(config-port-prof)# switchport mode trunk
Pod2-Nexus1000V(config-port-prof)# switchport trunk allowed vlan 1,20-21,50-51
Pod2-Nexus1000V(config-port-prof)# channel-group auto mode on mac-pinning
Pod2-Nexus1000V(config-port-prof)# no shutdown
Pod2-Nexus1000V(config-port-prof)# system vlan 1,20,21
Pod2-Nexus1000V(config-port-prof)# state enable
```

Configuring Other Important Port-Profiles

There are a couple important port-profiles which must be configured on the Cisco Nexus 1000V before we can migrate the hosts. This section will go through examples of creating a port-profile for the Service Console, VMotion traffic and iSCSI traffic. The network administrator will configure these port-profiles on the Nexus 1000V VSM which will push the port-profiles to vCenter where the server administrator can use vCenter to migrate the respective interfaces from the vSwitch to the Cisco Nexus 1000V.

CREATING A PORT-PROFILE FOR SERVICE CONSOLE

The name of this port-profile will be "Service-Console."

```
Pod2-Nexus1000V(config)# port-profile Service-Console
Pod2-Nexus1000V(config-port-prof)# switchport mode access
Pod2-Nexus1000V(config-port-prof)# switchport access vlan 200
Pod2-Nexus1000V(config-port-prof)# no shut
Pod2-Nexus1000V(config-port-prof)# system vlan 200
Pod2-Nexus1000V(config-port-prof)# state enabled
Pod2-Nexus1000V(config-port-prof)# vmware port-group
```

The “system VLAN configuration” is mandatory for all the virtual Interface that need to be up and running regardless of VSM to VEM connectivity. For example, the Service Console interface or the iSCSI interface both need to be up regardless if the Virtual Supervisor Module gets reloaded or becomes unreachable. The system VLAN configuration ensures that the specified VLAN will always be up and forwarding and must be included in the appropriate port-profiles as well as the uplink port-profiles.

CREATING A PORT-PROFILE FOR VMOTION

The name of this port-profile will be “VMotion.”

```
Pod2-Nexus1000V(config)# port-profile VMotion
Pod2-Nexus1000V(config-port-prof)# switchport mode access
Pod2-Nexus1000V(config-port-prof)# switchport access vlan 20
Pod2-Nexus1000V(config-port-prof)# no shut
Pod2-Nexus1000V(config-port-prof)# state enabled
Pod2-Nexus1000V(config-port-prof)# vmware port-group
```

Because VMotion cannot operate without at least one VSM being available, the system VLAN configuration is not mandatory for a VMotion port-profile.

CREATING A PORT-PROFILE FOR iSCSI

The name of this port-profile will be “iSCSI.”

```
Pod2-Nexus1000V(config)# port-profile iSCSI
Pod2-Nexus1000V(config-port-prof)# switchport mode access
Pod2-Nexus1000V(config-port-prof)# switchport access vlan 21
Pod2-Nexus1000V(config-port-prof)# system vlan 21
Pod2-Nexus1000V(config-port-prof)# no shut
Pod2-Nexus1000V(config-port-prof)# state enabled
Pod2-Nexus1000V(config-port-prof)# vmware port-group
```

For iSCSI traffic, the system VLAN configuration is mandatory since ESX host always need access to the storage. Therefore, the “system vlan 21” command must be included in the port-profile for iSCSI interfaces.

Migrating the Physical Host to the Nexus 1000V

Before migrating the physical NICs from the vSwitch to the Nexus 1000V, the following steps should be completed:

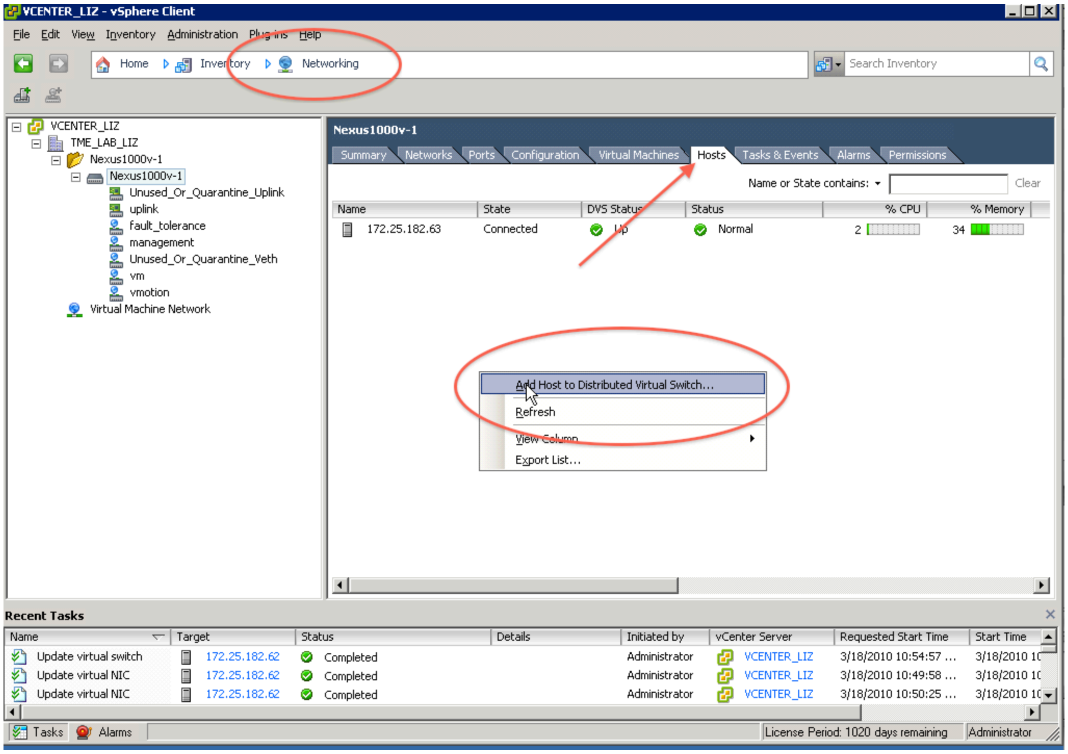
1. the correct port-profiles must be defined on the Nexus 1000V VSM. This includes the port-profiles for the physical interfaces as well as those for host virtual machines.
2. the upstream switch(s) are configured to trunk the appropriate VLANs down to the host including the management, control and packet VLANs.
3. the critical VLANs (management, control, packet, storage…) are declared as “system VLANs” within the port-profiles.

Once these steps are completed, it is possible to continue the migration process. There are three migration processes discussed in this section for migrating hosts to the Nexus 1000V: migration during the installation of the host, migration after the installation of the host, and migration with the use of VMware host-profiles.

Migrate the Interfaces During the Installation of the Host

Once all the port-profiles have been configured on the Nexus 1000V VSM, the migration can be done when adding the host to the Nexus 1000V distributed virtual switch. This is the only options for migrating the host if the deployment contains only a single physical uplink. The following steps outline how to add the host to the Nexus 1000V.

Step 1 Using VMware vSphere Client, browse to the **Networking** Tab, right click on the Nexus 1000V and select **Add Host**

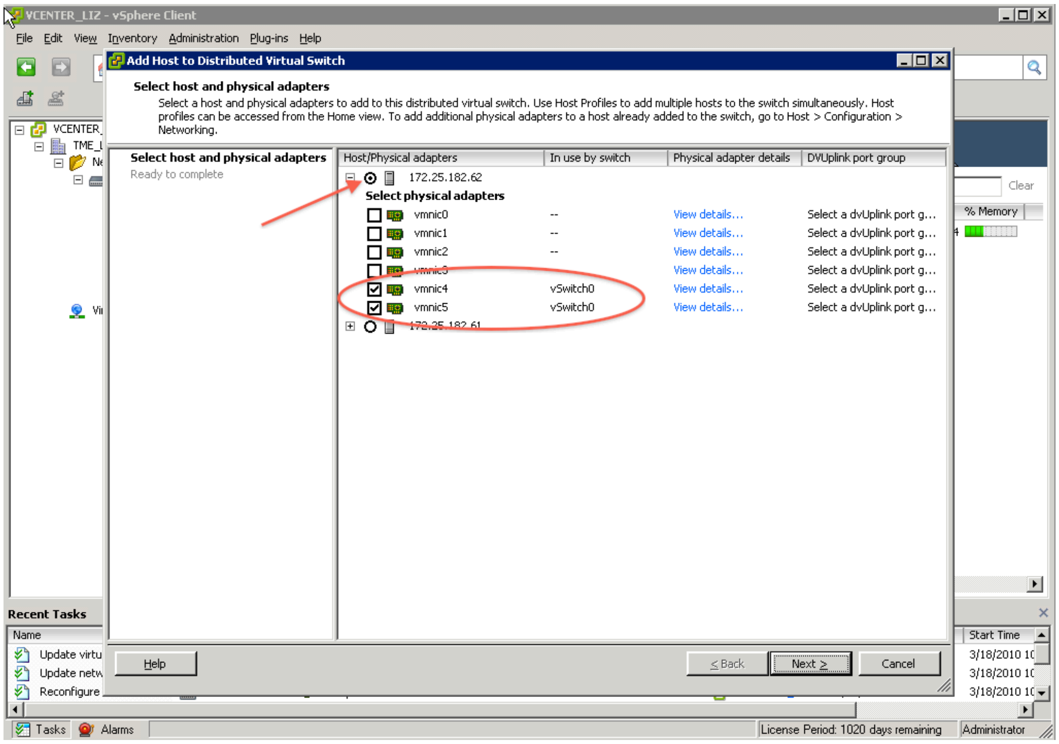


Name	State	DVS Status	Status	% CPU	% Memory
172.25.182.63	Connected	Up	Normal	2	34

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time
Update virtual switch	172.25.182.62	Completed		Administrator	VCENTER_LIZ	3/18/2010 10:54:57 …	3/18/2010 1
Update virtual NIC	172.25.182.62	Completed		Administrator	VCENTER_LIZ	3/18/2010 10:49:58 …	3/18/2010 1
Update virtual NIC	172.25.182.62	Completed		Administrator	VCENTER_LIZ	3/18/2010 10:50:25 …	3/18/2010 1

This will open the *Add Host to Distributed Virtual Switch Wizard*.

Step 2 Select the physical host that is being migrated as well as the vmnics being used by that host.



Add Host to Distributed Virtual Switch

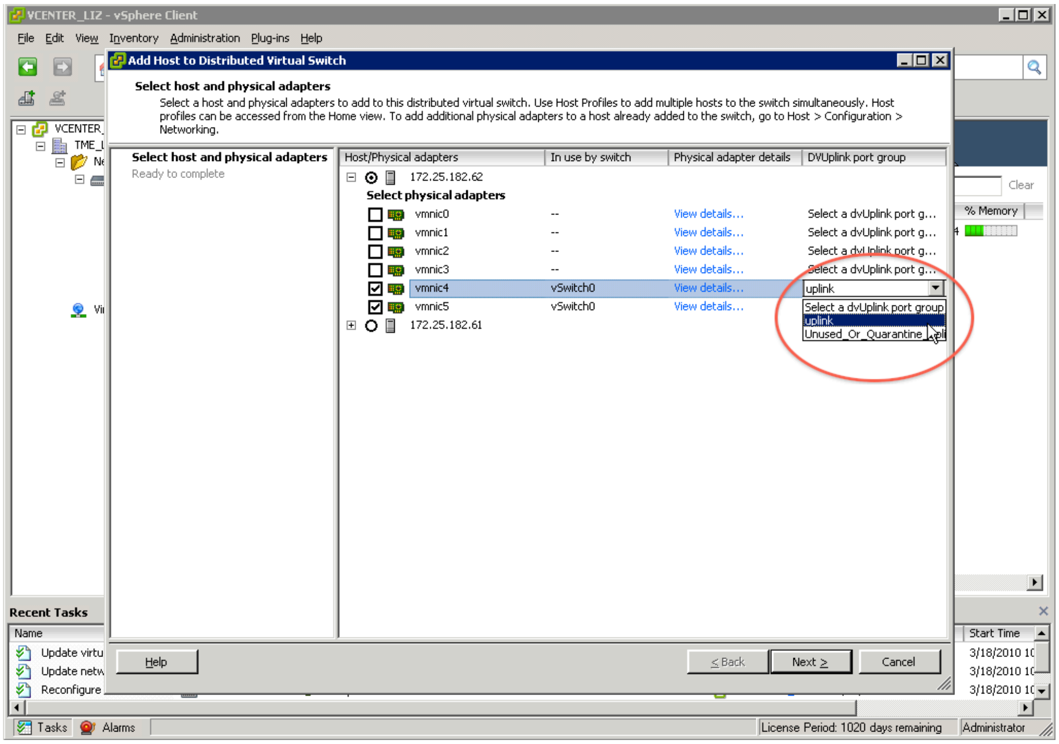
Select host and physical adapters

Select a host and physical adapters to add to this distributed virtual switch. Use Host Profiles to add multiple hosts to the switch simultaneously. Host profiles can be accessed from the Home view. To add additional physical adapters to a host already added to the switch, go to Host > Configuration > Networking.

Select host and physical adapters
Ready to complete

Host/Physical adapters	In use by switch	Physical adapter details	DVUplink port group
● 172.25.182.62			
Select physical adapters			
☐ vmnic0	--	View details...	Select a dvUplink port g...
☐ vmnic1	--	View details...	Select a dvUplink port g...
☐ vmnic2	--	View details...	Select a dvUplink port g...
☐ vmnic3		View details...	Select a dvUplink port g...
☑ vmnic4	vSwitch0	View details...	Select a dvUplink port g...
☑ vmnic5	vSwitch0	View details...	Select a dvUplink port g...
○ 172.25.182.61			

Step 3 Select the appropriate port-profiles for the individual vmnics from the drop down menu.


VCENTER_LIZ - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Add Host to Distributed Virtual Switch
Select host and physical adapters
Ready to complete
Help
< Back
Next >
Cancel
Recent Tasks
Name
Update virtu
Update netw
Reconfigure
Start Time
3/18/2010 1(
3/18/2010 1(
3/18/2010 1(
Clear
% Memory
Tasks
Alarms
License Period: 1020 days remaining
Administrator

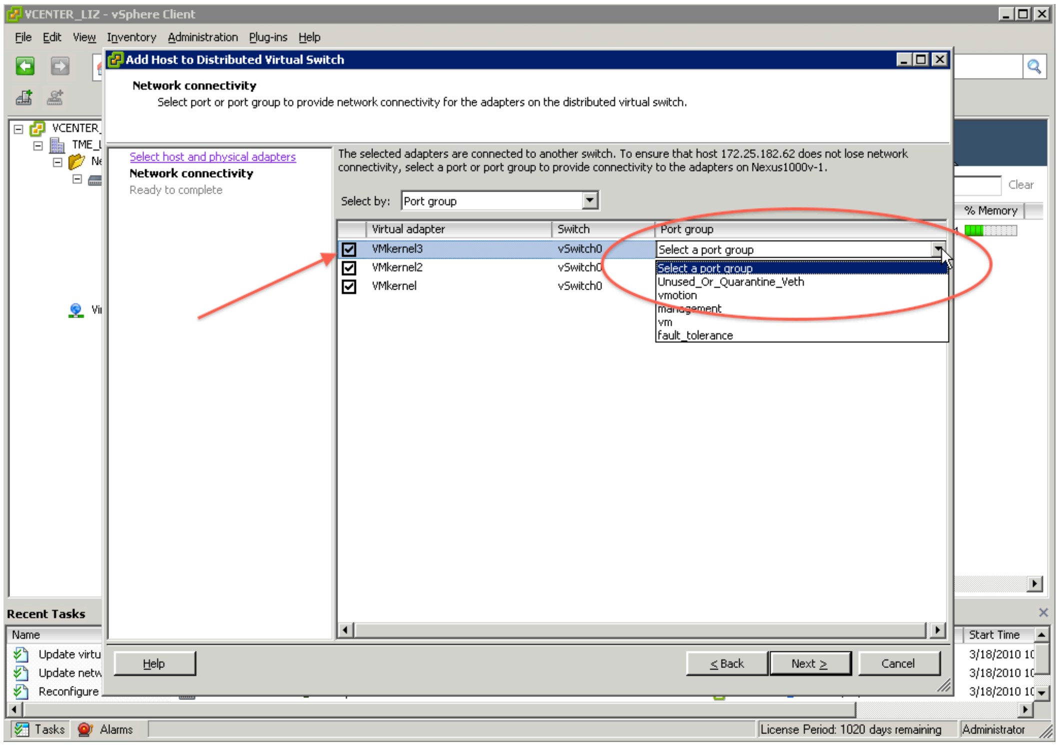
Select host and physical adapters

Select a host and physical adapters to add to this distributed virtual switch. Use Host Profiles to add multiple hosts to the switch simultaneously. Host profiles can be accessed from the Home view. To add additional physical adapters to a host already added to the switch, go to Host > Configuration > Networking.

Host/Physical adapters	In use by switch	Physical adapter details	DVUplink port group
● 172.25.182.62			
Select physical adapters			
☐ vmnic0	--	View details...	Select a dvUplink port g...
☐ vmnic1	--	View details...	Select a dvUplink port g...
☐ vmnic2	--	View details...	Select a dvUplink port g...
☐ vmnic3	--	View details...	Select a dvUplink port g...
☑ vmnic4	vSwitch0	View details...	uplink
☑ vmnic5	vSwitch0	View details...	
○ 172.25.182.61			

Select a dvUplink port group
uplink
Unused_Or_Quarantine_Upli

Step 4 VMware vCenter Client will prompt for the migration of the other virtual ports attached to the vswitch. Select the appropriate port-profile for each interface. Click **Next>** and then **Finish.**



Network connectivity

Select port or port group to provide network connectivity for the adapters on the distributed virtual switch.

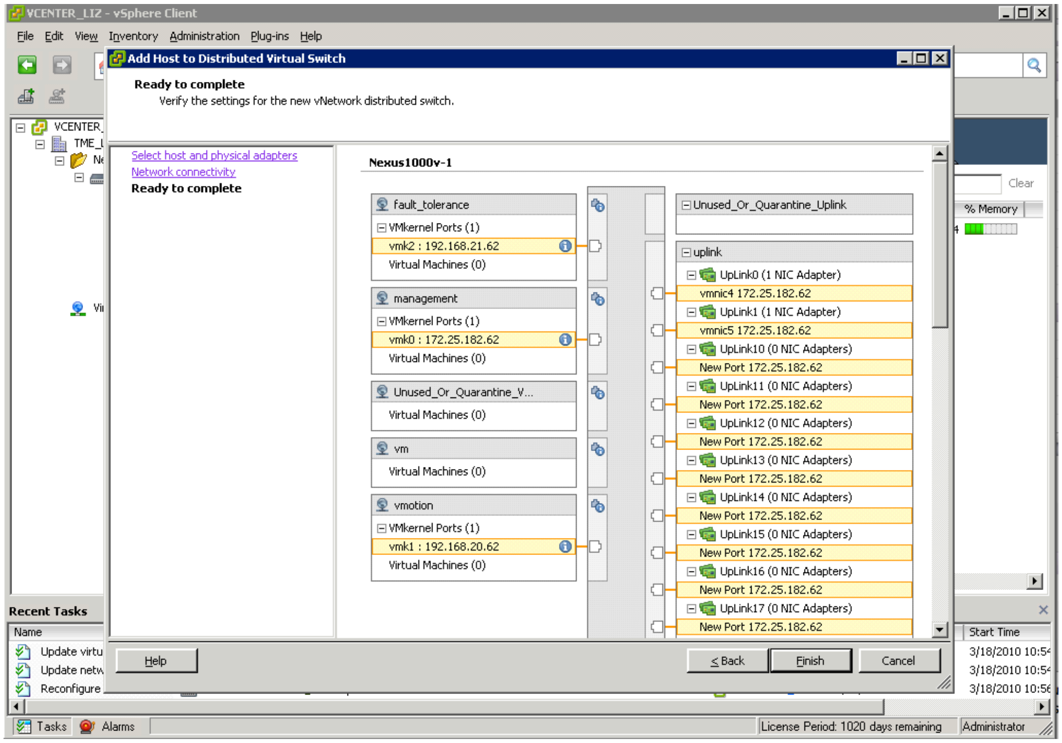
The selected adapters are connected to another switch. To ensure that host 172.25.182.62 does not lose network connectivity, select a port or port group to provide connectivity to the adapters on Nexus1000v-1.

Select by: Port group

Virtual adapter	Switch	Port group
☑ VMkernel3	vSwitch0	Select a port group
☑ VMkernel2	vSwitch0	
☑ VMkernel	vSwitch0	

Select a port group
Unused_Or_Quarantine_Veth
vmotion
management
vm
fault_tolerance

Step 5 Validate the new network settings and select finish to execute the add host operation.

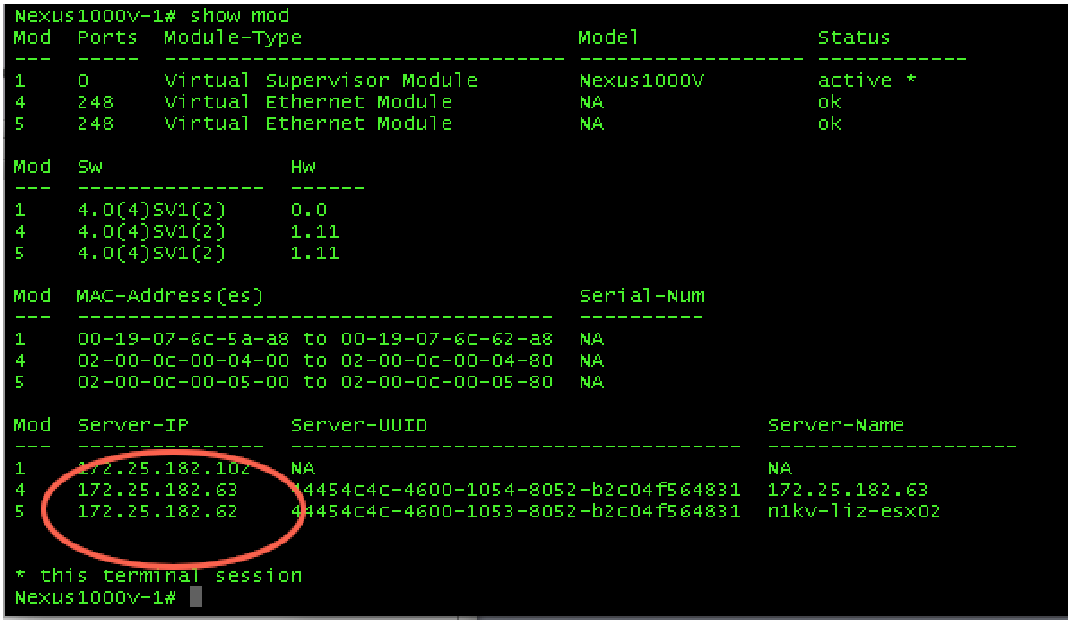


Add Host to Distributed Virtual Switch

Ready to complete

Verify the settings for the new vNetwork distributed switch.

Once this step is complete, VMware Update Manager (VUM) will automatically install the Cisco Nexus 1000V VEM software onto the host. If VUM is not being used, the VEM of the Nexus 1000V can be manually downloaded and installed. Both of these options should complete successfully if the configuration is correct and the host should be seen from the Cisco 1000V VSM. The following output from the **show module** command run on the Cisco Nexus 1000V VSM can be used to verify the migration of the host to the Cisco Nexus 1000V.

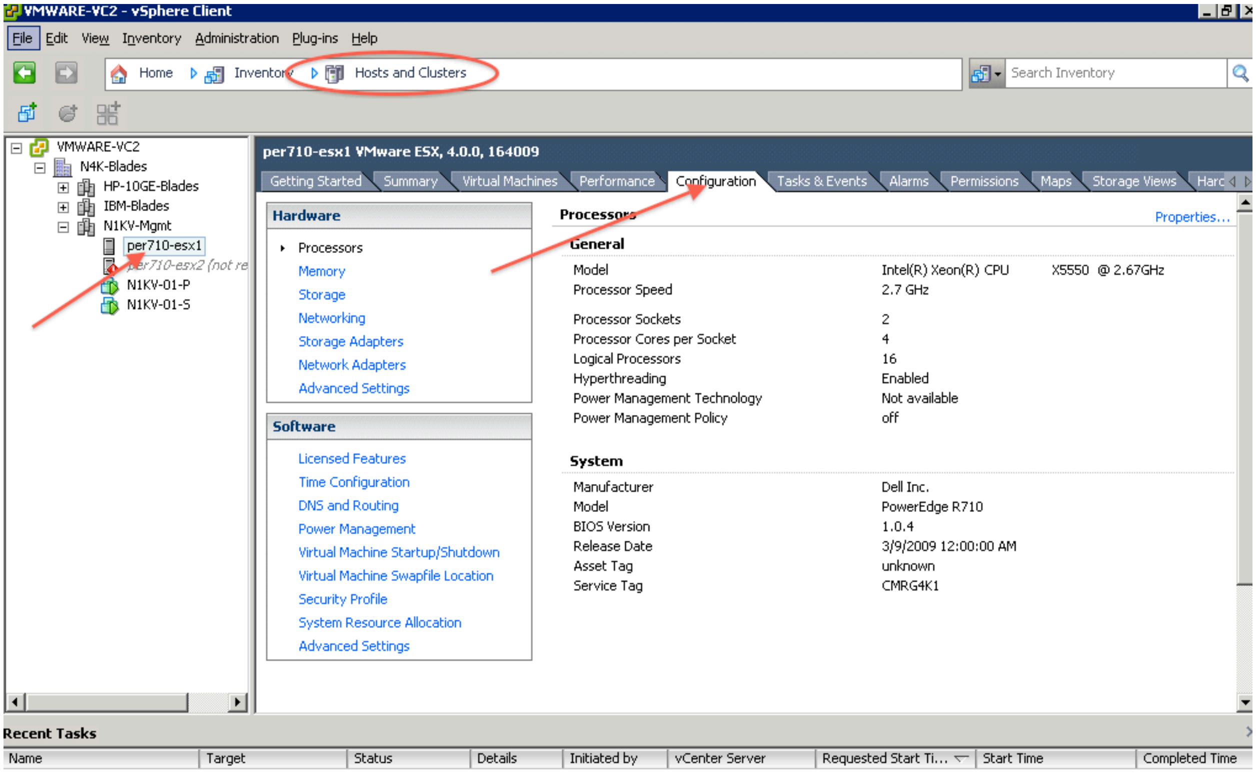


```
Nexus1000v-1# show mod
Mod  Ports  Module-Type                       Model              Status
---  -----  --------------------------------  -----------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V         active *
4    248    Virtual Ethernet Module           NA                 ok
5    248    Virtual Ethernet Module           NA                 ok

Mod  Sw                Hw
---  ----------------  ------
1    4.0(4)SV1(2)      0.0
4    4.0(4)SV1(2)      1.11
5    4.0(4)SV1(2)      1.11

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA
5    02-00-0c-00-05-00 to 02-00-0c-00-05-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    172.25.182.102   NA                                    NA
4    172.25.182.63    44454c4c-4600-1054-8052-b2c04f564831  172.25.182.63
5    172.25.182.62    44454c4c-4600-1053-8052-b2c04f564831  n1kv-liz-esx02


* this terminal session
Nexus1000v-1#
```

This migration process can also be completed in partial steps if the user is worried about possible connectivity complications. In order to be safe, users can chose to select a subset of the vmnics to migrate to the Nexus 1000V first. Once the host gets added to the DVS and the VEM gets installed on the host, the rest of the vmnics can be migrated over. This can reduce the risk of management connectivity loss.

Migrating the Interfaces After a Host is Added

Step 1 Using VMware vSphere Client, browse to the **Host and Clusters** Tab, click on the host name and then the **Configuration** tab



per710-esx1 VMware ESX, 4.0.0, 164009

Processors

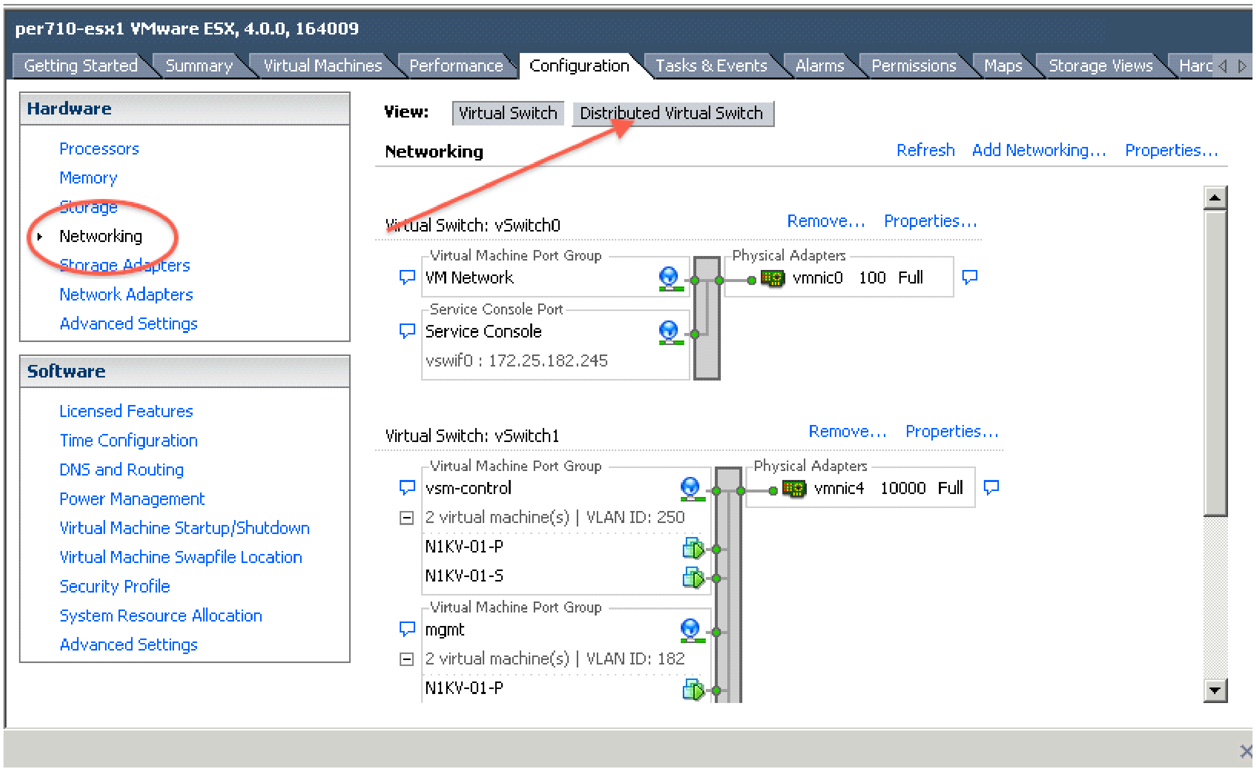
General

Model	Intel(R) Xeon(R) CPU X5550 @ 2.67GHz
Processor Speed	2.7 GHz
Processor Sockets	2
Processor Cores per Socket	4
Logical Processors	16
Hyperthreading	Enabled
Power Management Technology	Not available
Power Management Policy	off

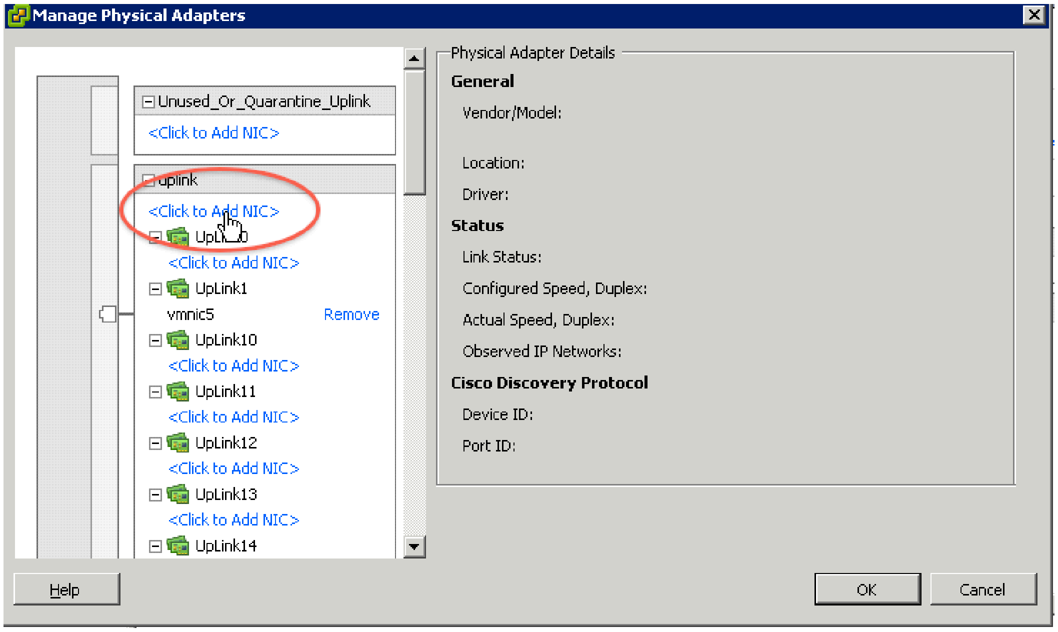
System

Manufacturer	Dell Inc.
Model	PowerEdge R710
BIOS Version	1.0.4
Release Date	3/9/2009 12:00:00 AM
Asset Tag	unknown
Service Tag	CMRG4K1

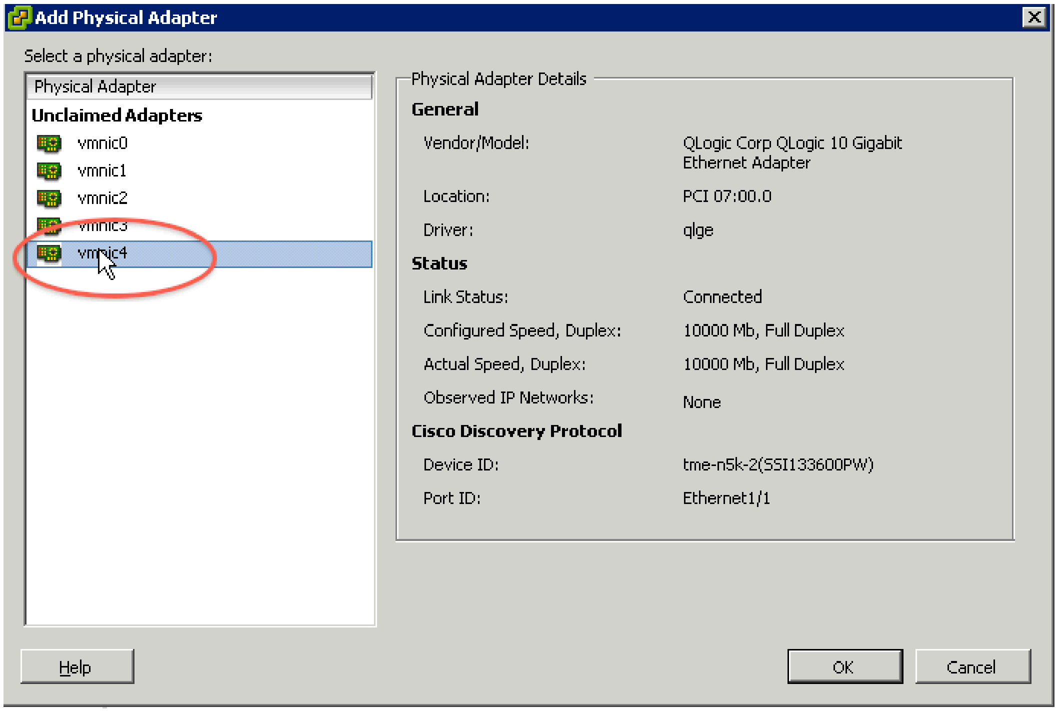
Step 2 Choose **Networking** from the left menu pane, click on **Distributed Virtual Switch**



Step 3 Click on **Manage Physical Adapter** to bring up this box and select **<Click to Add NIC>** found under the correct port-profile



Step 4 The **Add Physical Adapter** box will pop up. Select the vmnics under the correct vswitch and click **OK**. This will bring up a confirmation dialog box. Click **YES** and click **OK**



Physical Adapter Details

General

Vendor/Model: QLogic Corp QLogic 10 Gigabit Ethernet Adapter

Location: PCI 07:00.0

Driver: qlge

Status

Link Status: Connected

Configured Speed, Duplex: 10000 Mb, Full Duplex

Actual Speed, Duplex: 10000 Mb, Full Duplex

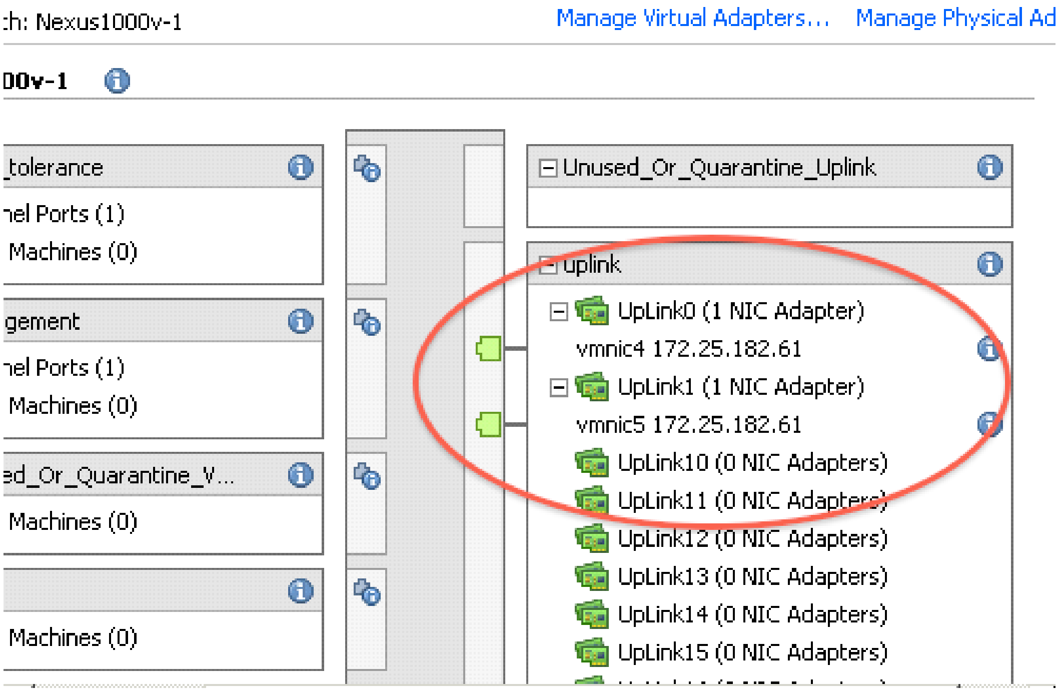
Observed IP Networks: None

Cisco Discovery Protocol

Device ID: tme-n5k-2(SSI133600PW)

Port ID: Ethernet1/1

Step 5 Verify that the adapters have been added to the Nexus 1000V

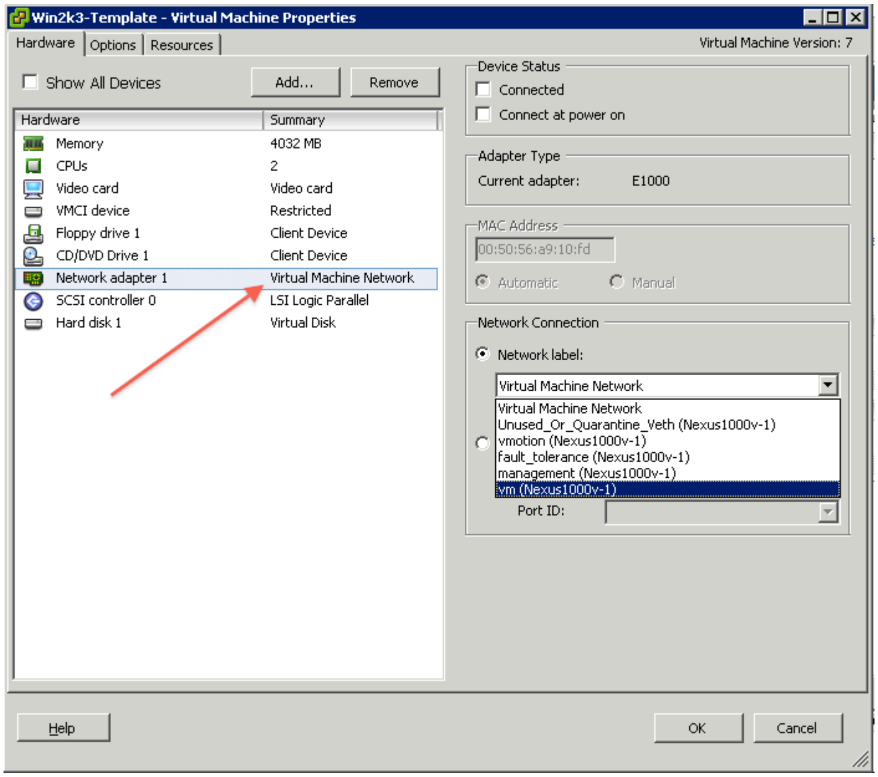


Migrating the Virtual Ports

Once the Nexus 1000V Virtual Ethernet Module is active on a host, it is recommended to migrate virtual ports and virtual machine uplinks from the VMware vSwitch to the VEM. This will help to ensure a consistent networking experience. All virtual ports, including those used for management (vswif0 on ESX, vmk0 on ESXi) as well as the management uplinks (if this wasn't completed in the previous process), as well as the virtual port belonging to the Nexus 1000V VSM. This section specifies procedures for migrating these ports, starting from a configuration that is created by the basic installation as specified in the Software Install Guide.

Migrate the Virtual Machine Interfaces to the Nexus 1000V

Step 1 Right-click on the VM and select **Edit Settings**. This brings up a dialog box where you can select the network adapter that needs to be migrated.


Win2k3-Template - Virtual Machine Properties
Hardware
Options
Resources
Virtual Machine Version: 7
☐ Show All Devices
Add...
Remove
Help
OK
Cancel

Hardware	Summary
Memory	4032 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
Floppy drive 1	Client Device
CD/DVD Drive 1	Client Device
Network adapter 1	Virtual Machine Network
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk

Device Status
☐ Connected
☐ Connect at power on

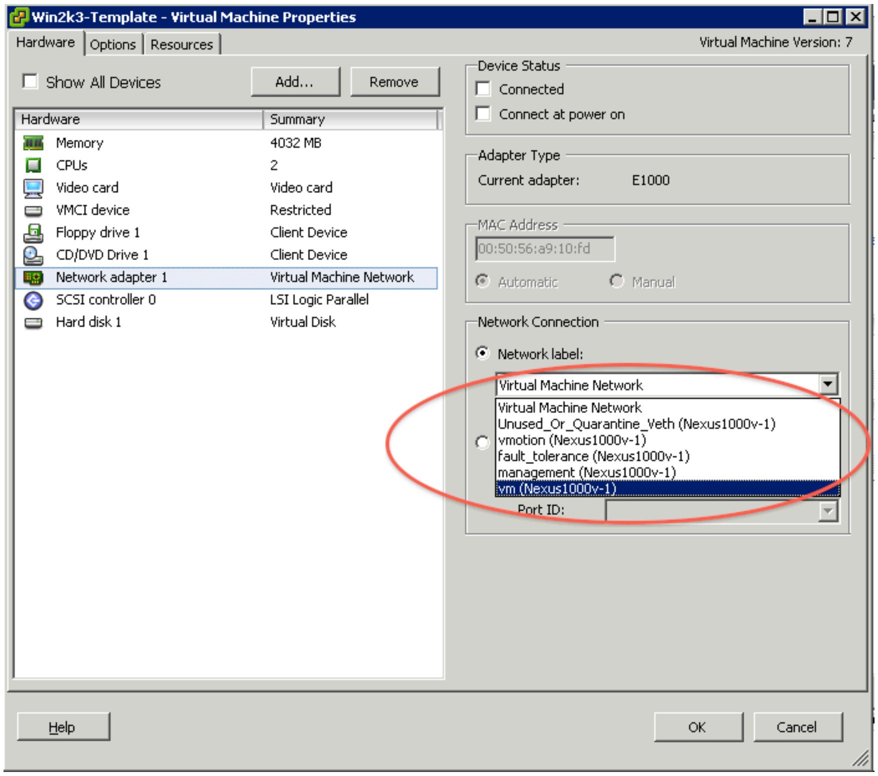
Adapter Type
Current adapter: E1000

MAC Address
00:50:56:a9:10:fd
● Automatic ○ Manual

Network Connection
● Network label:
Virtual Machine Network

Virtual Machine Network
Unused_Or_Quarantine_Veth (Nexus1000v-1)
vmotion (Nexus1000v-1)
fault_tolerance (Nexus1000v-1)
management (Nexus1000v-1)
vm (Nexus1000v-1)
○
Port ID:

Step 2 Select the correct pre–configured port-profile from the drop down list and select **OK**



Virtual Machine Version: 7

☐ Show All Devices

Hardware	Summary
Memory	4032 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
Floppy drive 1	Client Device
CD/DVD Drive 1	Client Device
Network adapter 1	Virtual Machine Network
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk

Device Status
☐ Connected
☐ Connect at power on

Adapter Type
Current adapter: E1000

MAC Address
00:50:56:a9:10:fd
● Automatic ○ Manual

Network Connection
● Network label:
Virtual Machine Network
Virtual Machine Network
Unused_Or_Quarantine_Veth (Nexus1000v-1)
vmotion (Nexus1000v-1)
fault_tolerance (Nexus1000v-1)
management (Nexus1000v-1)
vm (Nexus1000v-1)
○ Port ID:

Migrating the VSM virtual machine from vSwitch to Nexus 1000V

It is recommended to migrate the three virtual ports of the VSM VM from the vSwitch to either the Nexus 1000V VEM that it controls or another instance of the Cisco Nexus 1000V. The procedure for doing this is the same as migrating a virtual port that is described above. However, there is one important provision that must be taken into account: the profiles which are used for the VSM virtual machine must be system profiles where the control, packet and management VLANs are declared as “system VLANs” within the profile.

Migrating with the use of Host Profiles

Host profiles are a feature introduced by VMware in ESX 4.0.0 (Update 1) that allows users to create a profile that encapsulates the host configuration and helps manage the host configuration. This is especially useful in environments where a user manages more than one host or cluster in VMware vCenter Server. Host profiles eliminate per-host, manual or UI-based host configuration and helps to maintain configuration consistency and correctness across the datacenter.

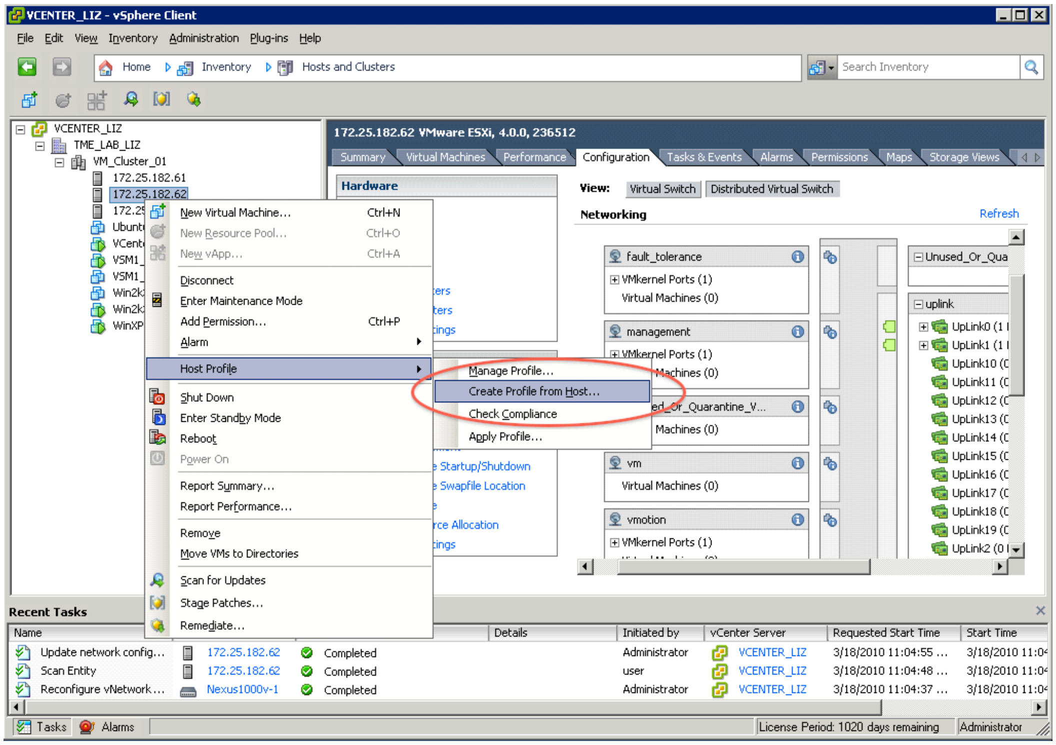
When a host profile is applied, the host will automatically be added to the distributed virtual switch. This can be used to ease the migration process from the vSwitch to the Cisco Nexus 1000V. By using host profiles we are able to take a “snapshot” of a migrated host and use that as a template to apply to other hosts in order to migrate them to the Nexus 1000V. The following section describes how to use host profiles in the migration from the vSwitch to the Nexus 1000V.

Before starting the migration process, it is suggested that a host profile be made which captures all of the ports attached to the vSwitch. This would be a "before snapshot" of the host living on the vSwitch and can be used if a situation comes up where the process needs to be reversed. Once this is complete, the first host must be migrated manually following the process above. Once a single host has gone through the migration process and is living on the Cisco Nexus 1000V, a host profile can be created of the migrated host. This host profile will capture all the necessary configuration of that physical ESX/ESXi host including the configuration that has moved the host to reside on the Nexus 1000V. This same profile can then be applied to all other hosts as well as future hosts that users want to migrate to the Cisco Nexus 1000V.

By using host profiles, users no longer have to migrate every host to the Nexus 1000V individually. Instead, users have the option of creating a host profile of a migrated host and simply applying that profile to all hosts that need to be migrated. This greatly simplifies the migration process.

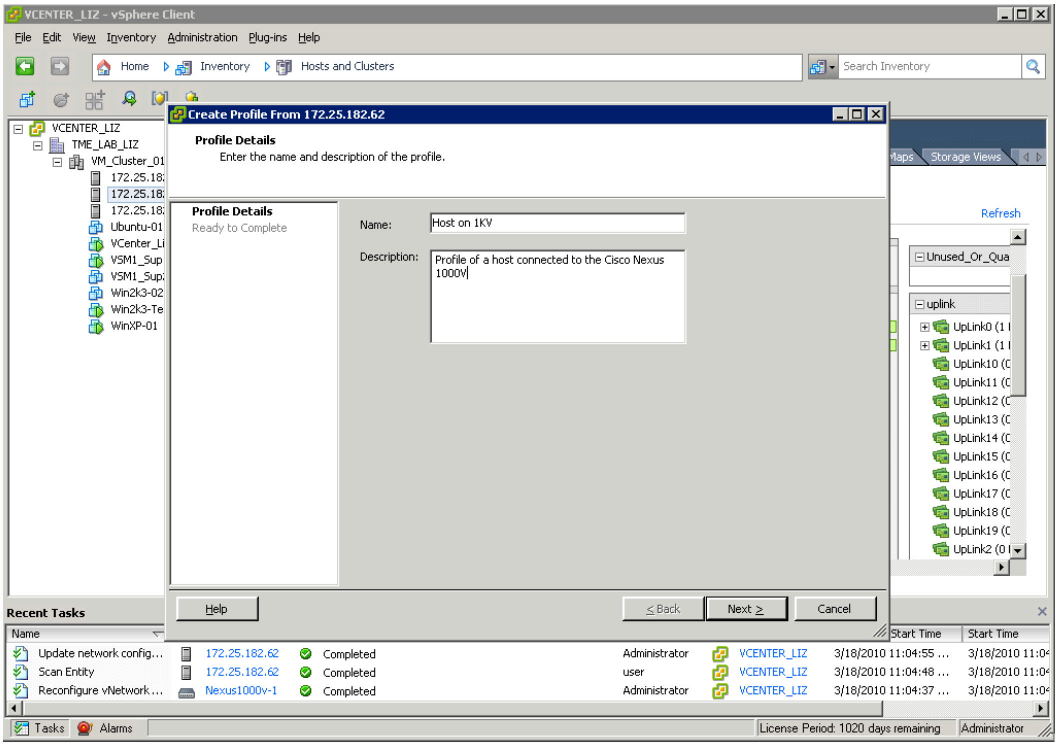
The creation of a host profile is shown in the following steps.

Step 1 Scroll to the **Hosts and Clusters** tab. Right-click on the host that will be used to make the port-profile. Scroll down toe **Host Profile** and select **Create Profile from Host…**



Name			Details	Initiated by	vCenter Server	Requested Start Time	Start Time
Update network config…	172.25.182.62	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:04:55 …	3/18/2010 11:0
Scan Entity	172.25.182.62	Completed		user	VCENTER_LIZ	3/18/2010 11:04:48 …	3/18/2010 11:0
Reconfigure vNetwork…	Nexus1000v-1	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:04:37 …	3/18/2010 11:0

Step 2 The **Create Profile From…** window will pop up. Instert a name and description of the host profile and click **Next>**



Create Profile From 172.25.182.62

Profile Details

Enter the name and description of the profile.

Profile Details
Ready to Complete

Name: Host on 1KV

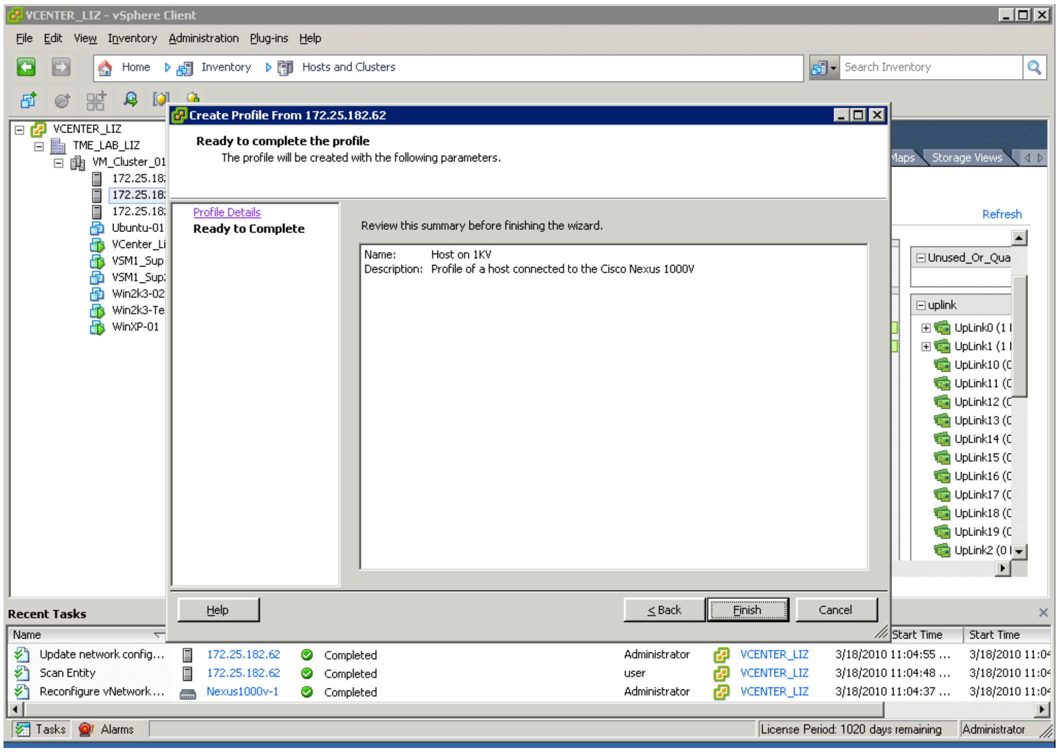
Description: Profile of a host connected to the Cisco Nexus 1000V

Recent Tasks

Name					Start Time	Start Time
Update network config...	172.25.182.62	Completed	Administrator	VCENTER_LIZ	3/18/2010 11:04:55 ...	3/18/2010 11:0
Scan Entity	172.25.182.62	Completed	user	VCENTER_LIZ	3/18/2010 11:04:48 ...	3/18/2010 11:0
Reconfigure vNetwork ...	Nexus1000v-1	Completed	Administrator	VCENTER_LIZ	3/18/2010 11:04:37 ...	3/18/2010 11:0

License Period: 1020 days remaining | Administrator

Step 3 Verify that the Name and Description and set appropriately and click **Finish** to create the host profile



Create Profile From 172.25.182.62

Ready to complete the profile

The profile will be created with the following parameters.

Profile Details
Ready to Complete

Review this summary before finishing the wizard.

Name: Host on 1KV
Description: Profile of a host connected to the Cisco Nexus 1000V

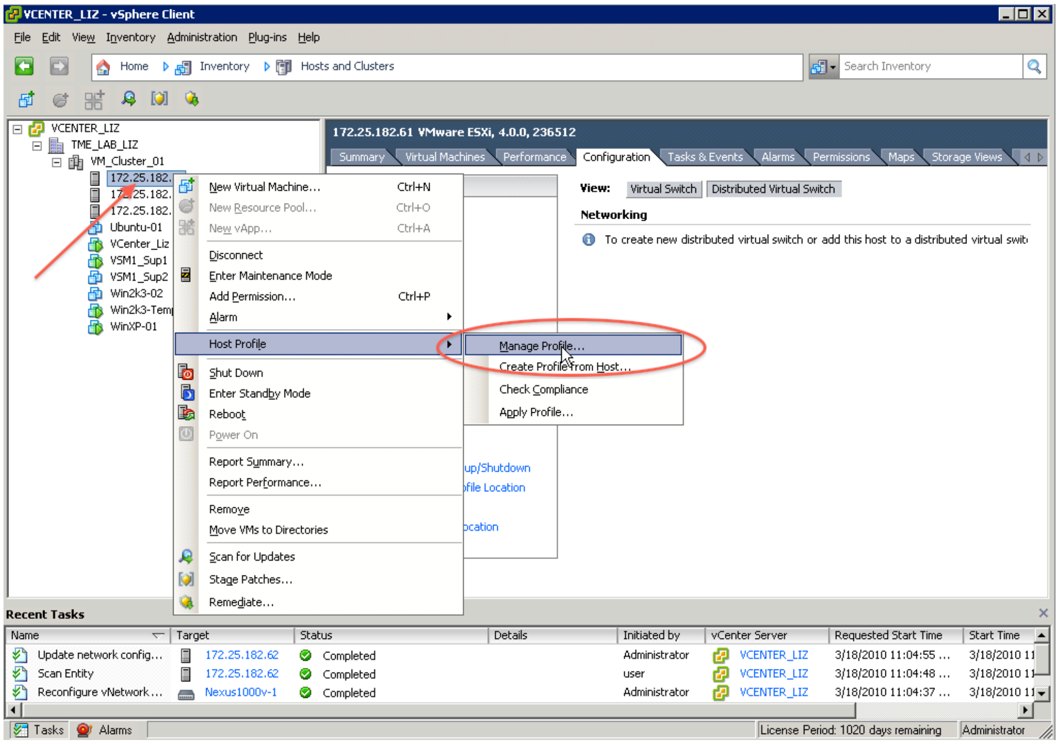
Recent Tasks

Name					Start Time	Start Time
Update network config...	172.25.182.62	Completed	Administrator	VCENTER_LIZ	3/18/2010 11:04:55 ...	3/18/2010 11:0
Scan Entity	172.25.182.62	Completed	user	VCENTER_LIZ	3/18/2010 11:04:48 ...	3/18/2010 11:0
Reconfigure vNetwork ...	Nexus1000v-1	Completed	Administrator	VCENTER_LIZ	3/18/2010 11:04:37 ...	3/18/2010 11:0

License Period: 1020 days remaining | Administrator

In order to apply a host profile, execute the following steps:

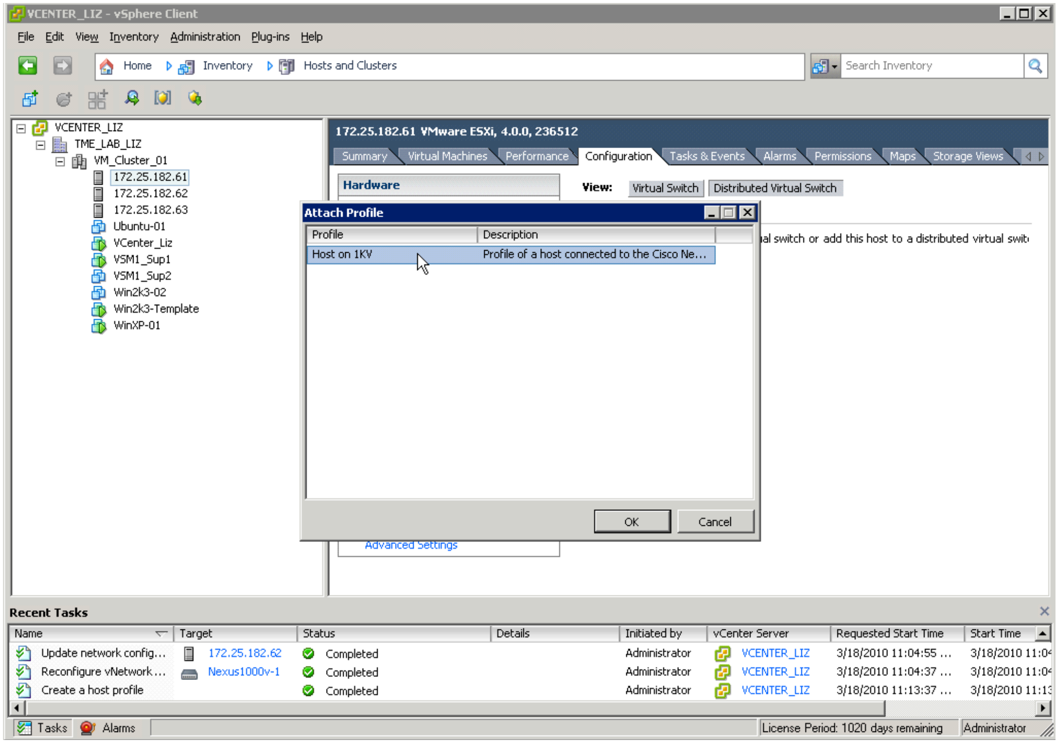
Step 1 Scroll to the **Hosts and Clusters** tab. Right-click on the host that will inherit the host profile, scroll down to **Host Profile** and select **Manage Profile…**



To create new distributed virtual switch or add this host to a distributed virtual swit

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time
Update network config…	172.25.182.62	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:04:55 …	3/18/2010 11
Scan Entity	172.25.182.62	Completed		user	VCENTER_LIZ	3/18/2010 11:04:48 …	3/18/2010 11
Reconfigure vNetwork…	Nexus1000v-1	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:04:37 …	3/18/2010 11

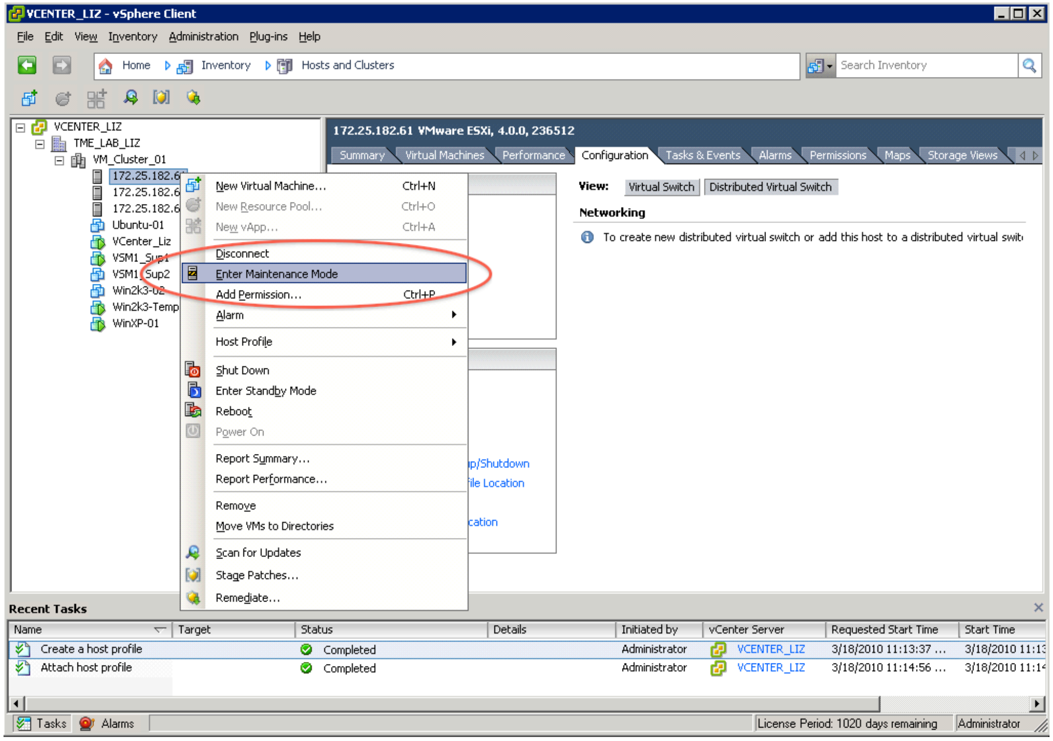
Step 2 Select the host profile which is going to be applied and click **OK**


VCENTER_LIZ - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
VCENTER_LIZ
TME_LAB_LIZ
VM_Cluster_01
172.25.182.61
172.25.182.62
172.25.182.63
Ubuntu-01
VCenter_Liz
VSM1_Sup1
VSM1_Sup2
Win2k3-02
Win2k3-Template
WinXP-01
172.25.182.61 VMware ESXi, 4.0.0, 236512
Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permissions Maps Storage Views
Hardware
View: Virtual Switch Distributed Virtual Switch
al switch or add this host to a distributed virtual swit
Attach Profile
OK
Cancel
Advanced Settings
Recent Tasks
Tasks Alarms
License Period: 1020 days remaining
Administrator

Profile	Description
Host on 1KV	Profile of a host connected to the Cisco Ne…

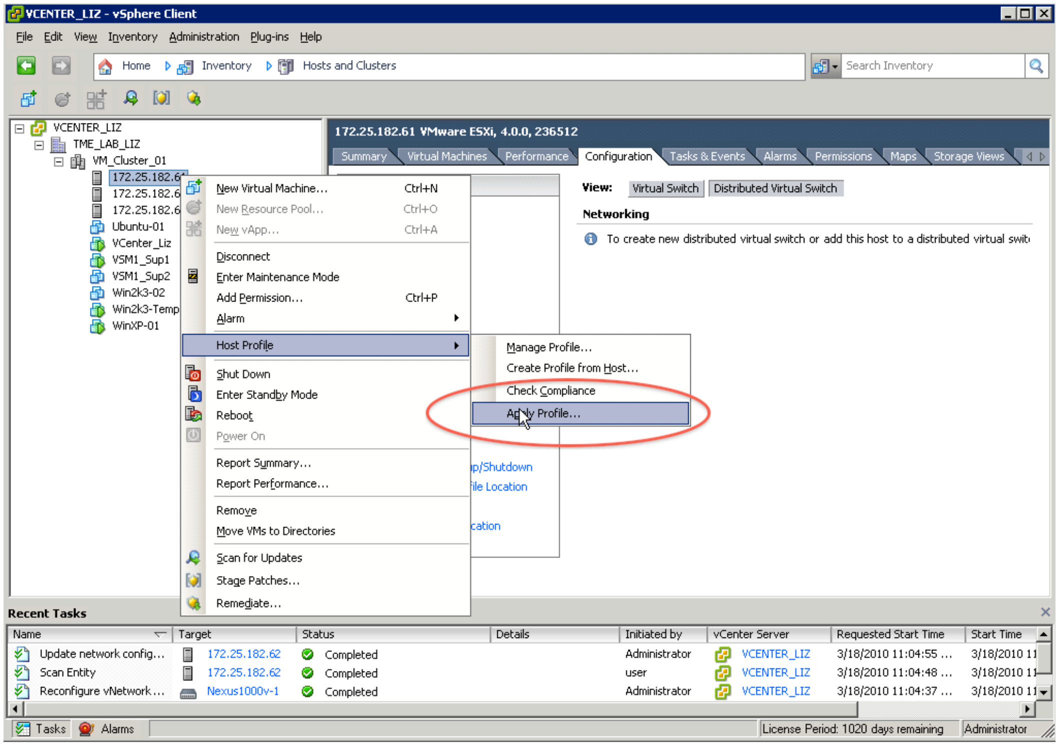
Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time
Update network config…	172.25.182.62	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:04:55 …	3/18/2010 11:0
Reconfigure vNetwork…	Nexus1000v-1	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:04:37 …	3/18/2010 11:0
Create a host profile		Completed		Administrator	VCENTER_LIZ	3/18/2010 11:13:37 …	3/18/2010 11:1

Step 3 Right-click on the host that will inherit the host profile, and put the host in **Maintenance Mode**


VCENTER_LIZ - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
VCENTER_LIZ
TME_LAB_LIZ
VM_Cluster_01
172.25.182.6
172.25.182.6
172.25.182.6
Ubuntu-01
VCenter_Liz
VSM1_Sup1
VSM1_Sup2
Win2k3-02
Win2k3-Temp
WinXP-01
172.25.182.61 VMware ESXi, 4.0.0, 236512
Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permissions Maps Storage Views
New Virtual Machine… Ctrl+N
New Resource Pool… Ctrl+O
New vApp… Ctrl+A
Disconnect
Enter Maintenance Mode
Add Permission… Ctrl+P
Alarm
Host Profile
Shut Down
Enter Standby Mode
Reboot
Power On
Report Summary…
Report Performance…
Remove
Move VMs to Directories
Scan for Updates
Stage Patches…
Remediate…
View: Virtual Switch Distributed Virtual Switch
Networking
To create new distributed virtual switch or add this host to a distributed virtual swit
p/Shutdown
ile Location
cation
Recent Tasks
Tasks Alarms
License Period: 1020 days remaining
Administrator

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time
Create a host profile		Completed		Administrator	VCENTER_LIZ	3/18/2010 11:13:37 …	3/18/2010 11:1
Attach host profile		Completed		Administrator	VCENTER_LIZ	3/18/2010 11:14:56 …	3/18/2010 11:1

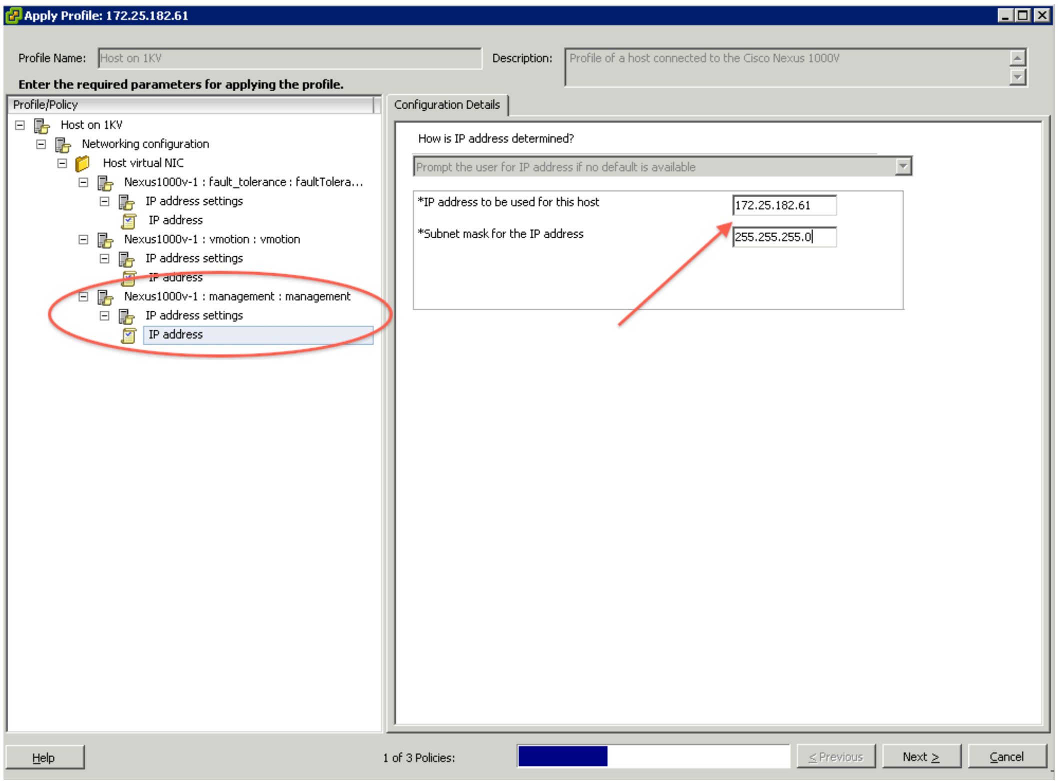
Step 4 Once the host is in maintenance mode, right-click on that host and scroll down to **Host Profile** and choose **Apply Profile**



To create new distributed virtual switch or add this host to a distributed virtual swit

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time
Update network config...	172.25.182.62	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:04:55 ...	3/18/2010 11
Scan Entity	172.25.182.62	Completed		user	VCENTER_LIZ	3/18/2010 11:04:48 ...	3/18/2010 11
Reconfigure vNetwork...	Nexus1000v-1	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:04:37 ...	3/18/2010 11

Step 5 Depending on the type and number of vmknics configured on the host, a window may pop up asking for the parameters that should be used. Enter the necessary information and click **Next>**



Profile Name: Host on 1KV

Description: Profile of a host connected to the Cisco Nexus 1000V

Enter the required parameters for applying the profile.

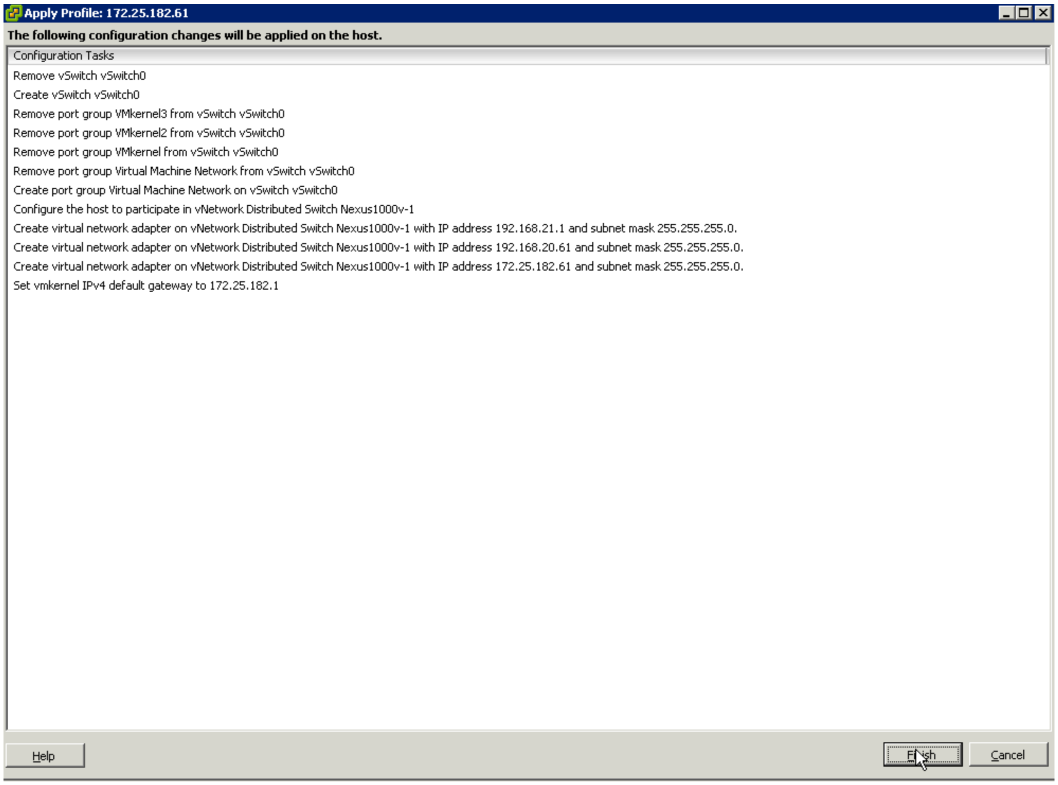
How is IP address determined? Prompt the user for IP address if no default is available

*IP address to be used for this host: 172.25.182.61

*Subnet mask for the IP address: 255.255.255.0

.

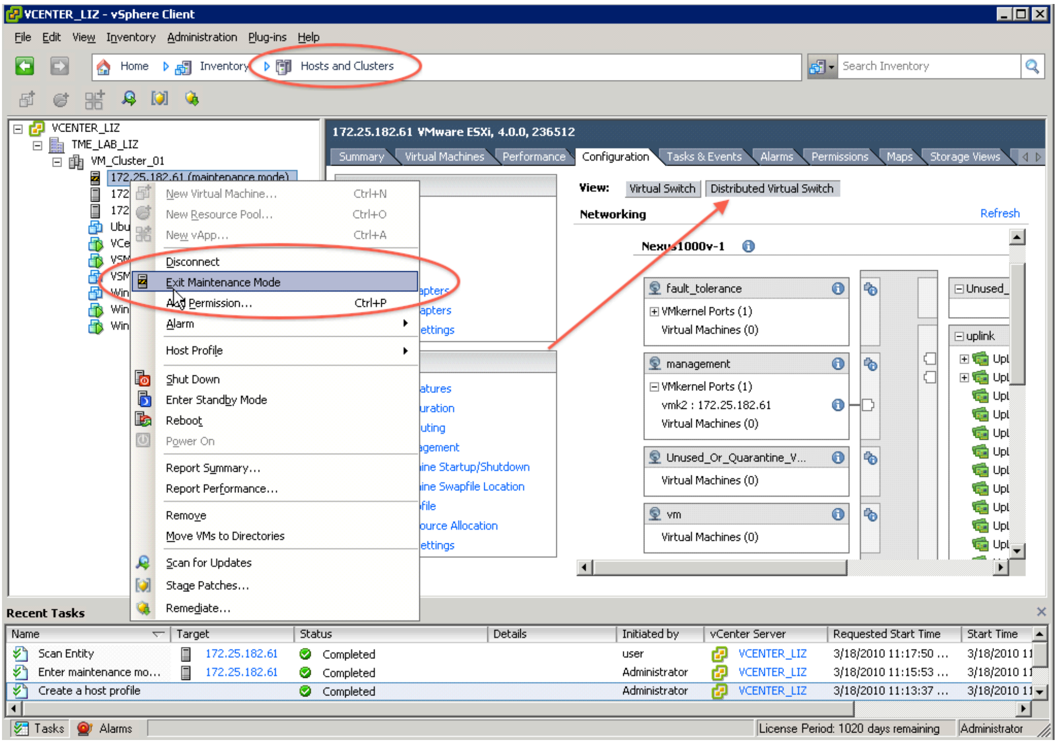
Step 6 Verify the paramters and configuration that will be applied to the host



The following configuration changes will be applied on the host.

Remove vSwitch vSwitch0
Create vSwitch vSwitch0
Remove port group VMkernel3 from vSwitch vSwitch0
Remove port group VMkernel2 from vSwitch vSwitch0
Remove port group VMkernel from vSwitch vSwitch0
Remove port group Virtual Machine Network from vSwitch vSwitch0
Create port group Virtual Machine Network on vSwitch vSwitch0
Configure the host to participate in vNetwork Distributed Switch Nexus1000v-1
Create virtual network adapter on vNetwork Distributed Switch Nexus1000v-1 with IP address 192.168.21.1 and subnet mask 255.255.255.0.
Create virtual network adapter on vNetwork Distributed Switch Nexus1000v-1 with IP address 192.168.20.61 and subnet mask 255.255.255.0.
Create virtual network adapter on vNetwork Distributed Switch Nexus1000v-1 with IP address 172.25.182.61 and subnet mask 255.255.255.0.
Set vmkernel IPv4 default gateway to 172.25.182.1

Step 7 Right click on the host and select **Exit Maintenance Mode**. Verify that the host was successfully migrated to the Nexus 1000V by clicking on the **Configuration** tab and selecting the **Distributed Virtual Switch**

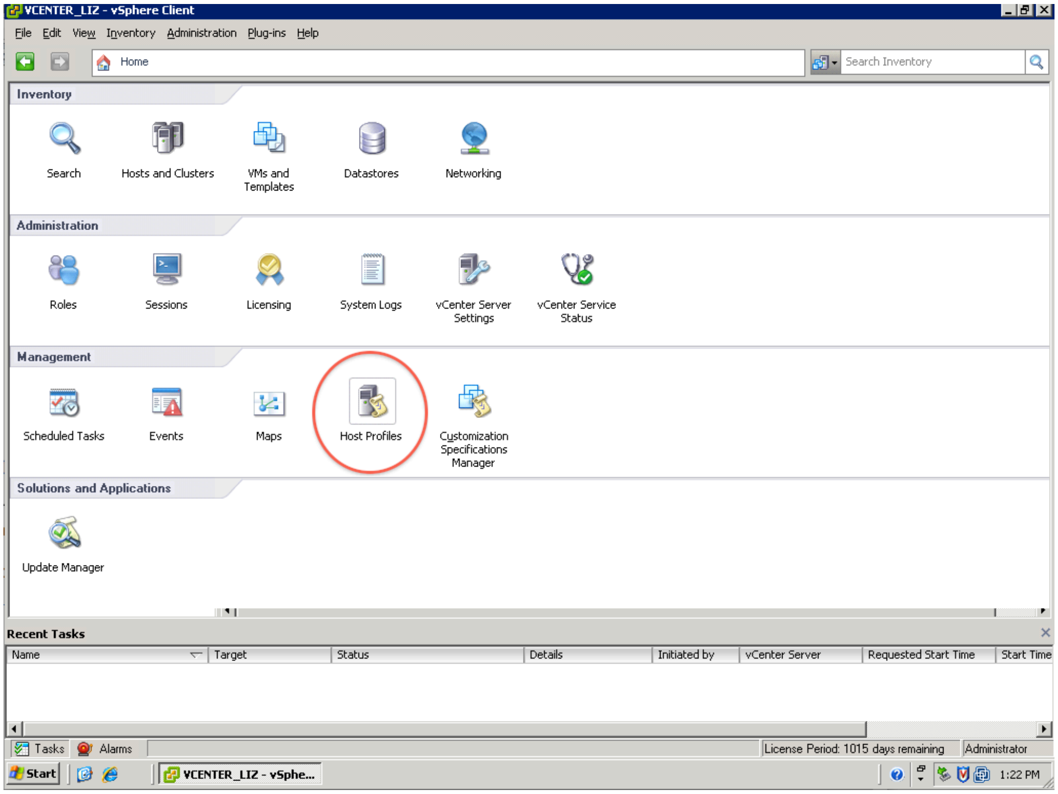


Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time
Scan Entity	172.25.182.61	Completed		user	VCENTER_LIZ	3/18/2010 11:17:50 ...	3/18/2010 11
Enter maintenance mo...	172.25.182.61	Completed		Administrator	VCENTER_LIZ	3/18/2010 11:15:53 ...	3/18/2010 11
Create a host profile		Completed		Administrator	VCENTER_LIZ	3/18/2010 11:13:37 ...	3/18/2010 11

Host Profile Considerations

There are a couple of considerations to take into account when using VMware's Host Profiles as a way to migrate hosts from the vSwitch to the Nexus 1000V.

1. In a mixed environment consisting of both ESX and ESXi hosts, it is possible to apply a Host Profiles taken from an ESX host to an ESXi host. However, if applying a profile taken from an ESXi host to an ESX host, the profile needs to be edited so that the ESX host will know which vmknic to use for management. Host profiles can be edited by scrolling to the **Home** page and selecting **Host Profiles** from the **Management** menu.



2. When applying host profiles in an environment where there are multiple types of physical Network Interface Cards (NICs) deployed, issues may arise from the differences in supported parameters for the various NICs i.e. auto-negotiation. In the case where supported parameters differ between the various NICs, it is suggested that the host profile be edited in order to comply.