WHITE PAPER

VMware® vNetwork Distributed Switch: Migration and Configuration

vmware®

Table of Contents

Introduction 3
Purpose of this Guide 3
What is a vNetwork Distributed Switch? 3
Configuration and Deployment Scenarios 3
Hybrid vSS/vDS/Nexus Virtual Switch Environments 4
Scale 4
VMWare® VMotion™ and VMware® Network VMotion 4
VMotion Domain Considerations 4
Port Assignments in Hybrid vSS and vDS Environments . . . 4
DV Port Groups and DV Uplink Port Groups. 4
Single vDS. 5
Multiple vDS 6
Cisco Nexus 1000V Scenarios. 7
Planning the Migration to vDS 7
Host Migration with some Disruption to VMs 9
Host Migration without Disruption to VMs. 9
Applying NIC Teaming Policies to DV Port Groups 10
Guided Example of Migration from a vNetwork Standard Switch to a vNetwork Distributed Switch 11
NIC Teaming Configuration. 14
VLAN Assignment. 15
Considerations for vDS Migration. 15
Creation and Migration Overview. 16
Creation and Migration Process. 16
Step 1: Create a vDS 16
What is an Uplink Group?. 17
Step 2: Create Distributed Virtual Port Groups on vDS to Match Existing or Required Environment 17
What is a Distributed Virtual Port Group? 17
Port Group to DV Port Group Mappings. 17
Creating the DV Port Groups 18
Step 3: Add host to vDS and migrate vmnics, Virtual Ports, and VM Networking 19
Step 3a: Add Host to vDS. 19
Step 3c: Migrate Virtual Adapters 19
Step 4: Repeat Step 3 for Remaining Hosts. 22
Step 5: Optionally Delete Standard Switches from Hosts . 22
Step 6: Adjusting Distributed Virtual Port Groups Policies 23
Editing DV Port Group Policies. 23
How vDS Helps with Policy Adjustments. 24
Summary of vDS UI Migration Method. 24
Considerations for using Host Profiles for Deploying vDS24
Process Overview 24
Step 1 to Step 4: Migrate Reference Host to vDS 25
Step 5: Create Host Profile of Reference Host 25
Step 6: Attach and Apply Host Profile to Candidate Hosts 26
Step 7: Migrate VM Networking to vDS 28
Changes using the Standard Switch 29
Changes using the vNetwork Distributed Switch 29
Monitoring, Troubleshooting, and Recovery 31
Configuring CDP. 34
Monitoring Hash vmnic Selection in NIC Teams 34
ESXi Host Virtual Network Recovery 36

Introduction

The VMware® vNetwork Distributed Switch (vDS) is a new type of virtual switch introduced with VMware vSphere™ 4. The vDS simplifies virtual machine networking by enabling you to manage virtual machine networking for a number of hosts in a datacenter as a single virtual switch from a centralized VMware vCenter™ Server through a vSphere client interface.

Purpose of this Guide

This guide is intended to help the reader migrate from an environment using vNetwork Standard Switches to one using vNetwork Distributed Switches. It assumes the environment has already been upgraded to vSphere 4 and VMware® ESX™ 4 with the applicable level of licensing for vDS.

What is a vNetwork Distributed Switch?

A vNetwork Distributed Switch is an aggregation of per-host virtual switches presented and controlled as a single distributed switch through vCenter Server at the Datacenter level. The vDS abstracts configuration of individual virtual switches and enables centralized provisioning, administration, and monitoring.

Configuration and Deployment Scenarios

Physical and virtual network implementations vary from site to site. In this section various vDS deployment scenarios are explored assuming starting point of vNetwork Standard Switches on ESX 4 and VMware ESX™ i 4 hosts, typical of a newly upgraded environment.

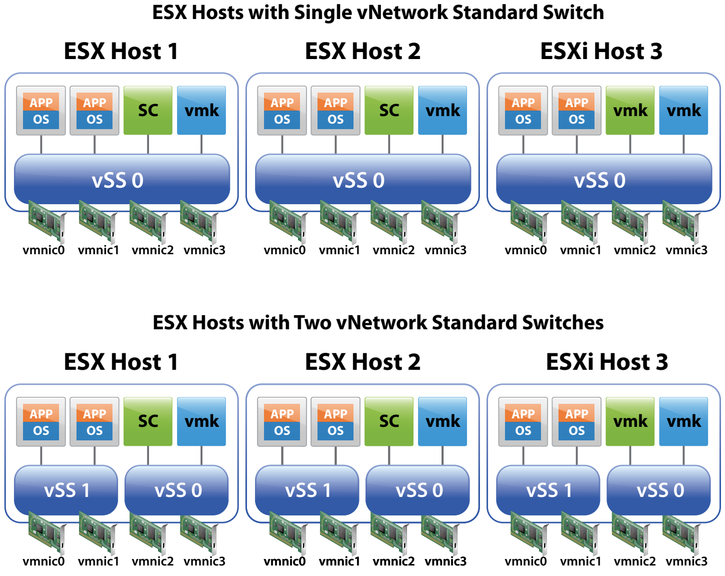
Pre-Migration Environment with vNetwork Standard Switches

Most VMware Infrastructure 3 (VI3) virtual network environments are deployed using one or two virtual switches (vSwitches) on each host as shown in Figure 1. The virtual networking environment would appear similar upon an upgrade to vSphere 4 (note that vSwitches are called vNetwork Standard Switches (abbreviated to vSS) in vSphere 4). This is the starting point for migration to vDS in the description and examples that follow.

These environments are further characterized by the following:

- VLANs used to separate traffic with 802.1Q trunking on uplinks (VST or Virtual Switch Trunking mode)
- NIC teaming policies implemented at vSwitch and Port Group level to maximize availability and load balancing
- May use a combination of ESX and ESXi hosts

Figure 1 - Typical deployment scenario with one or two vSwitches or vNetwork Standard Switches per host.



Configuration Considerations for the vNetwork Distributed Switch

The vDS follows many of the same configuration conventions and rules as the vNetwork Standard Switch. A vDS can span multiple hosts within a vCenter Server Datacenter construct.

Hybrid vSS/vDS/Nexus Virtual Switch Environments

Each ESX host can concurrently operate a mixture of virtual switches as follows:

- One or more vNetwork Standard Switches
- One or more vNetwork Distributed Switches
- A maximum of one Cisco Nexus 1000V (VEM or Virtual Ethernet Module).

Note that physical NICs (vmnics) cannot be shared between virtual switches (i.e. each vmnic only be assigned to one switch at any one time).

Scale

Scaling maximums should be considered when migrating to a vDS. The following virtual network configuration maximums are supported in the first release of vSphere 4:

- 64 ESX/ESXi Hosts per vDS
- 16 Distributed Switches (vDS or Nexus 1000V) per vCenter Server
- 512 Distributed Virtual Port Groups per vCenter Server
- 6000 Distributed Virtual Switch Ports per vCenter
- 4096 total vSS and vDS virtual switch ports per host

Note: These configuration maximums are subject to change. Consult the Configuration Maximums for vSphere 4 documents at vmware.com for the most current scaling information.

VMWare® VMotion™ and VMware® Network VMotion

VMware® Network VMotion is a feature included with vDS (and the Nexus 1000V) that preserves network port state when a Virtual Machine (VM) migrates from one host to another using VMotion. Network VMotion thus ensures network port statistics for individual VMs are consistent across VMotions. As network port state is preserved, Network VMotion is also a prerequisite for any stateful monitoring that might be added such as firewalls.

VMotion Domain Considerations

VMs attached to a vDS (a dvport on a vDS) can only migrate using VMotion to another port on the same vDS. Any host within the VMotion domain must share a common vDS.

Port Assignments in Hybrid vSS and vDS Environments

In a hybrid environment featuring a mixture of vNetwork Standard Switches and vNetwork Distributed Switches, VM networking should be migrated to vDS in order to take advantage of Network VMotion. As Service Consoles and VMkernel ports do not migrate from host to host, these can remain on a vSS. However, if you wish to use some of the advanced capabilities of the vDS for these ports, such as Private VLANs or bi-directional traffic shaping, or, team with the same NICs as the VMs (for example, in a two port 10GbE environment), then you will need to migrate all ports to the vDS.

DV Port Groups and DV Uplink Port Groups

DV Port Groups on vDS are configuration templates for a group of ports and have a similar function and purpose to Port Groups on a vSS. DV Port Groups span all the hosts covered by a vDS, so any configuration change to a DV Port Group is reflected on all hosts covered by that vDS. In addition to those parameters available on a vSS Port Group, a vDS DV Port Group supports the following items and policies:

- Traffic Shaping Policies. These policies apply to the dvPorts connecting the VMs and virtual ports (vmkernel ports, service console ports) and are relative to those ports.
  - Ingress Traffic Shaping governs the flow from the VM or virtual port to the vSwitch (vDS).

  - Egress Traffic Shaping governs the flow from the vSwitch (vDS) to the VM or virtual port.

- **VLAN Policy**. Specifies the VLAN type and number (if applicable) for dvports covered by that DV Port Group.
  - *None* — port is assigned to native VLAN (untagged traffic on uplinks when using VST mode) or same as uplinks ports (when in EST mode) indicating no VLAN tagging (uplinks are connected to access ports on physical switches.
  - *VLAN* — ports are assigned to that specific VLAN when virtual switch is in VST mode (VLAN tagged traffic on uplinks). This is the most common selection.
  - *VLAN Trunking* — traffic is passed through to Guest VM with VLAN tags intact (i.e. not stripped). (Under ESX 3.5 this option was selected and configured by specifying VLAN 4095).
  - *Private VLAN* — Private VLANs are a new feature of vDS that permit per Guest VM isolation on a shared IP subnet.

DV Uplink Port Groups are unique to vDS. They specify a subset of parameters that apply to the dvPorts and inherited by the DV Port Groups. The following items and policies can be defined on a DV Uplink Port Group:

- **Name of the dvUplink Port Group**. Name is automatically generated if not explicitly selected.
- **Traffic Shaping Policies**. These policies apply to the dvPorts connecting the VMs and virtual ports (vmkernel ports, service console ports) and are relative to those ports. The same rules apply for DV Port Groups and DV Uplink Port Groups:
  - Ingress Traffic Shaping governs the flow from the VM or virtual port to the vSwitch (vDS).
  - Egress Traffic Shaping governs the flow from the vSwitch (vDS) to the VM or virtual port.
- **VLAN**. This parameter governs VLAN connectivity on the DV Uplinks. In most cases where VLAN Trunking is used into the virtual switch from the adjacent physical switches (also known as VST mode or Virtual Switch Trunking), VLAN Trunking is selected as the VLAN type. The VLAN Trunk Range specifies what VLANs are permitted into the vDS from the physical network. This permits pruning of unnecessary VLANs. Specify the VLANs used on the all the DV Port Groups as a range or individual VLAN numbers. Specify 1-4094 to allow all VLANs without pruning.

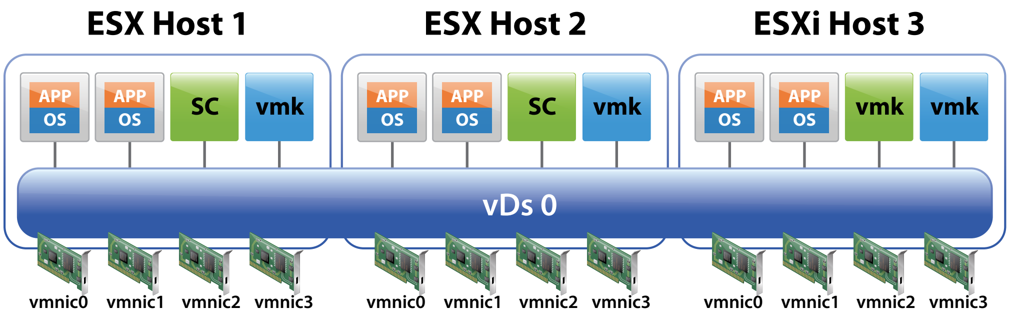
Example of Distributed Switch Configurations

A vDS can be deployed with or without vSS and/or a Nexus 1000V switch according to the rules and guidelines outlined above. This section presents some examples of these variations.

Single vDS

Migrating the entire vSS environment to a single vDS represents the simplest deployment and administration model. See Figure 2 below. All VM networking plus VMkernel and service console ports are migrated to the vDS. The NIC teaming policies configured on the DV Port Groups can isolate and direct traffic down the appropriate dvUplinks (which map to individual vmnics on each host).

Figure 2 - Single vDS Environment

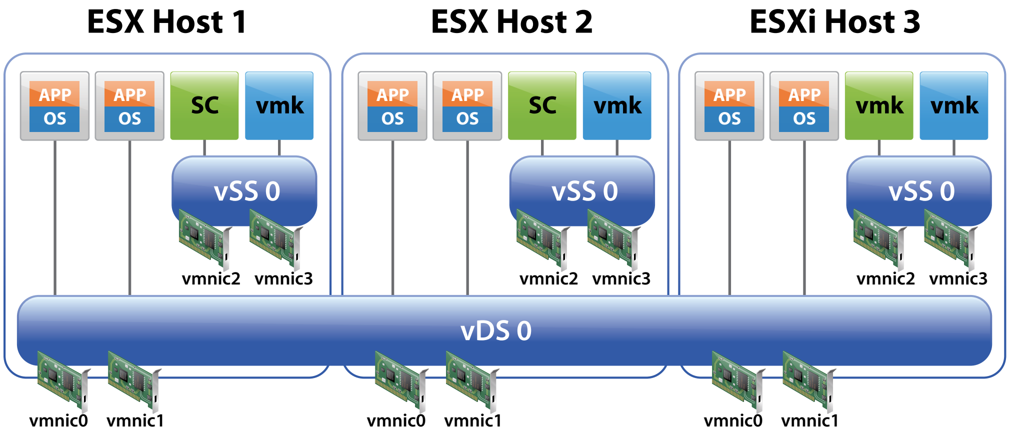


Hybrid vDS and vSS

Figure 3 shows an example environment where the VM networking is migrated to a vDS, but the Service Console and VMkernel ports remain on a vSS. This scenario might be preferred for some environments where the NIC teaming policies for the VMs are isolated from those of the VMkernel and Service Console ports. For example, in the diagram at the bottom of Figure 1, the vmnics and VM networks on vSS-1 could be migrated to vDS-0 in Figure 3, while vSS-0 could remain intact and in place.

In this scenario, VMs can still take advantage of Network VMotion as they are located on dv Port Groups on the vDS.

Figure 3 - Hybrid vDS and vSS Environment

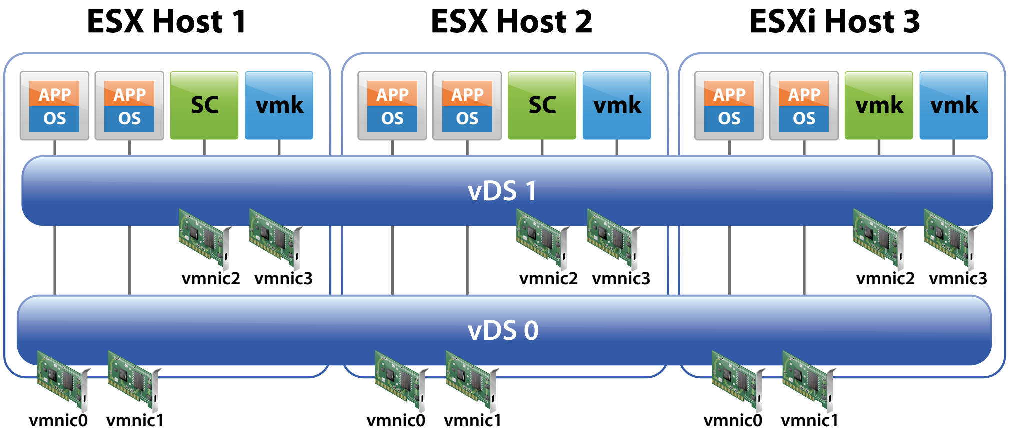


Multiple vDS

Hosts can be added to multiple vDS's as shown in Figure 4. (Two are shown, but more could be added, with or without vmnic to dvUplink assignments). This configuration might be used to:

1. Retain traffic separation when attached to access ports on physical switches (i.e. no VLAN tagging and switchports are assigned to a single VLAN).
2. Retain switch separation but use advanced vDS features for all ports and traffic types.

Figure 4 - Multiple vDS Environment



Cisco Nexus 1000V Scenarios

The Cisco Nexus 1000V exploits the third party virtual switch functionality of the vDS and follows the same distributed model as the vDS. Figure 6 shows the most common Nexus 1000V configuration with Figure 5 as additional hybrid alternative. A Nexus 1000V can also co-exist with a vDS and vSS, but this use case might be considered unusual except for cases of splitting virtual network administration between the network admin (Nexus 1000V) and server admin (vDS/vSS).

Figure 5 - Cisco Nexus 1000V with vSS Environment

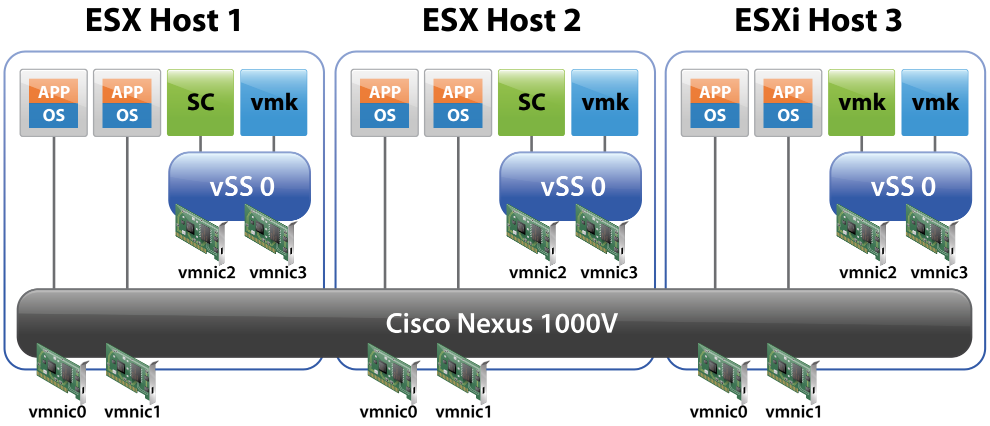
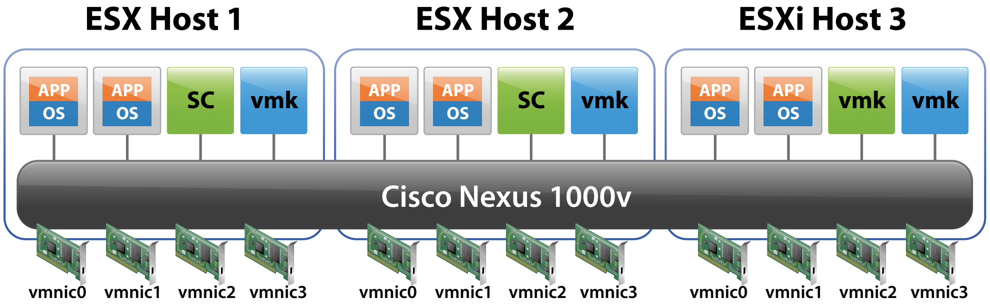


Figure 6 - Single Cisco Nexus 1000V Environment



Planning the Migration to vDS

Migration from a vNetwork Standard Switch only environment to one featuring one or more vNetwork Distributed Switches can be accomplished in either of two ways:

1. ***Using only the vDS User Interface (vDS UI***) — Hosts are migrated one by one by following the New vNetwork Distributed Switch process under the **Home > Inventory > Network** view of the Datacenter from the vSphere Client.
2. ***Using a combination of the vDS UI and Host Profiles***— The first host is migrated to vDS and the remaining hosts are migrated to vDS using a Host Profile of the first host.

Background to Using the vDS User Interface

The vDS UI is used to create vDS representation, dvUplinks, and DV Port Groups on the vCenter Server. After a vDS is created, hosts can be added, vmnics assigned to dvUplinks, virtual ports (VMkernels, Service Consoles) migrated, and virtual machine port groups migrated to the new vDS.

The vDS UI affords a fine level of control over the migration process. It allows per host control over the vmnic to dvUplinks assignments—critical for maintaining appropriate and intended NIC teaming policies when vmnic to physical switch connections vary from host to host.

The vDS UI also allows a phased migration of vmnics from vSS to vDS without disruption to an operational environment. VMs can be migrated from a vSS to a vDS on the fly so long as the vDS and vSS have connectivity to the same network at the same time and the origin Port Group on the vSS and destination DV Port Group on the vDS are configured to the same VLAN.

Background to Using Host Profiles

Host Profiles provide a way to migrate multiple hosts at one time. Host Profiles use a golden profile from a migrated host to propagate a configuration to a number of other hosts.

When applying a Host Profile to a host, the host must be in **Maintenance Mode**. This requires VMs to be either powered down or migrated to another host.

Host Profiles are most appropriate for new installations of similarly configured hosts (i.e. same number of vmnics, same vmnic to physical switch configuration, no active VMS).

Summary of Migration Methods

The table below summarizes the deployment situations and suggested methods for migration from vSS to vDS. Note: These are suggestions only; both methods will work within the guidelines mentioned above.

Table 1 - Summary of vSS to vDS Migration Methods

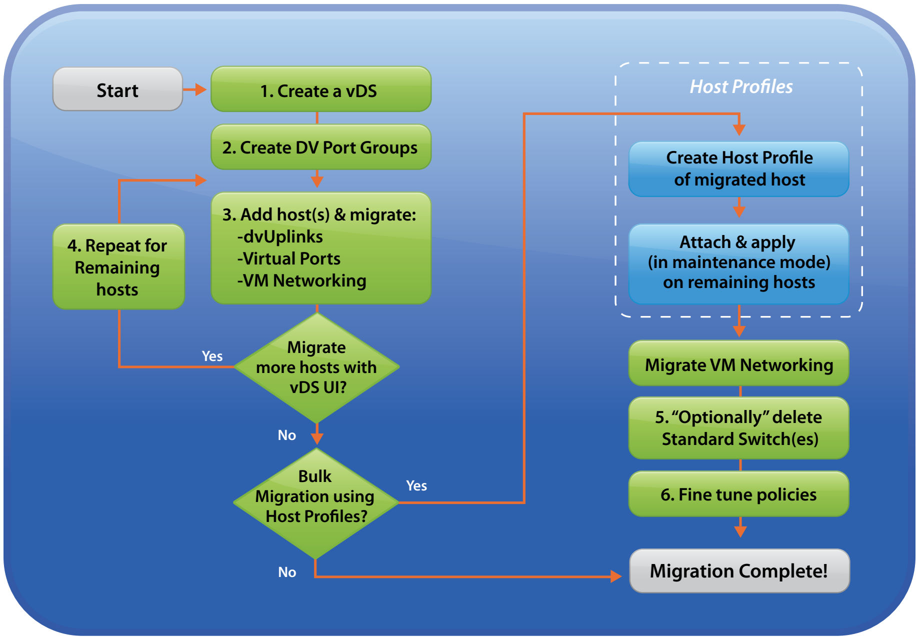
Deployment Situation	Suggested Method	Details
New servers, same vmnic config, no active VMs	vDS UI + HP	Migrate first host with vDS UI. Take host profile and apply to remaining hosts
<5 Existing Servers, no active VMs	vDS UI	Small number of servers. Can use host profiles, but possibly easier to continue with vDS UI
>5 Existing servers, same vmnic configs, no active VMs	vDS UI + HP	Larger number of servers with similar vmnic configuration. No active VMs so can enter maintenance mode and use Host Profiles
Existing Servers, active/operational VMs	vDS UI	Cannot use Maintenance Mode as VMs active. Phased vmnic migration suggested to ensure continuity of VM communications
Existing Servers, dissimilar vmnic configurations	vDS UI	Enables per host tailoring of vmnic to dvUplink PortGroup mapping
Ongoing Compliance Checking	HP	Non-disruptively check network settings are compliant with approved "golden" configuration

Note: vDS UI = Use vDS UI; HP = use Host Profiles; vDS + HP = use vDS UI to deploy first host and Host Profiles for remaining hosts

Migration Process

The flowchart in Figure 7 shows the migration process for migrating hosts to a vNetwork Distributed Switch.

Figure 7 - Flowchart of vSS to vDS Migration Process using vDS UI and Host Profiles


Start
1. Create a vDS
2. Create DV Port Groups
3. Add host(s) & migrate:
-dvUplinks
-Virtual Ports
-VM Networking
4. Repeat for Remaining hosts
Yes
Migrate more hosts with vDS UI?
No
Bulk Migration using Host Profiles?
Yes
No
Host Profiles
Create Host Profile of migrated host
Attach & apply (in maintenance mode) on remaining hosts
Migrate VM Networking
5. "Optionally" delete Standard Switch(es)
6. Fine tune policies
Migration Complete!

Some minor variations can be made to this process with the ordering of DV Port Group Creation, migration of VM Networking, and addition of hosts to a vDS (i.e. add now or add later).

Host Migration with some Disruption to VMs

The process as outlined in Step 3 of the flowchart includes two sub-steps:

A. Migration of vmnics and virtual ports (VMkernel ports and Service Consoles) can be migrated in a single step from vCenter Server.

B. Migration of VM Networking where the VMs are migrated from vSS Port Groups to vDS DV Port Groups.

If all vmnics are migrated in Step A, then all VMs will lose network connectivity until Step B. Step B can follow quickly after Step A (it is up to the speed of the operator), but active sessions will most likely drop. However, VMs can remain powered on.

Host Migration without Disruption to VMs

If you need a completely non-disruptive migration for VMs while deploying vDS, then a phased vmnic migration is required. The objective of a phased migration of vmnics is to maintain concurrent network connectivity over both vSS and vDS switches so that VM migration from vSS Port Groups to vDS DV Port Groups can proceed without interruption to network sessions.

Step 3 of the non-disruptive process is as follows:

A. Add host to vDS

B. Migrate one vmnic from the NIC team supporting VM networking from vSS to vDS dvUplink

C. Migrate VM networking from vSS Port Groups to vDS DV Port Groups

D. Migrate remaining vmnics and virtual ports (vmkernel and Service Consoles) to vDS

If you intend to keep a vSS and just migrate VM networking to vDS, then Step D will involve migrating the remaining vmnics from the VM networking nic teams to vDS dvUplinks.

Applying NIC Teaming Policies to DV Port Groups

With a vSS, NIC teaming policies are defined on the virtual switch with an optional override on each Port Group definition. With vDS, NIC teaming policies are only defined on the DV Port Groups and apply to dvUplinks, not vmnics. The vmnics are mapped to the dvUplinks on a per host basis. This enables each host to have a different vmnic to physical host configuration and yet use the same NIC teaming policy over all hosts spanned by the vDS.

It is perhaps easier and less troublesome to apply the NIC teaming policies to the DV Port Groups after the migration is complete (Step 6 shown in flowchart).

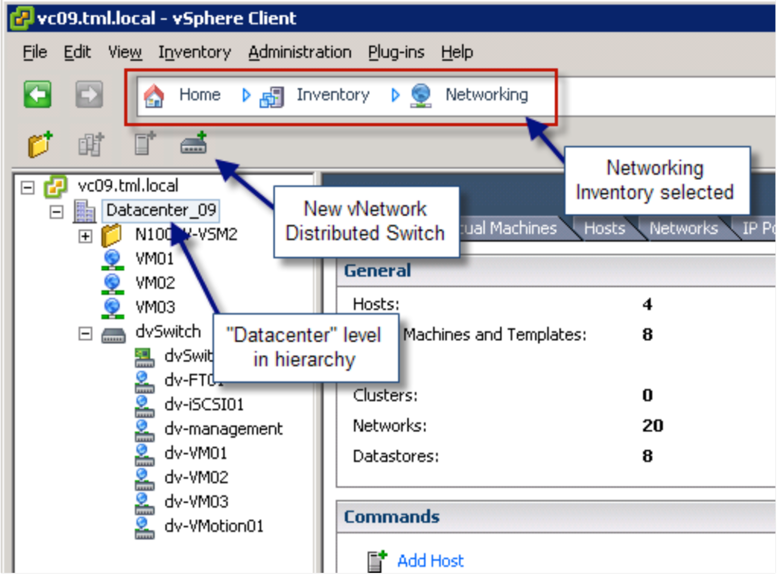
Using the vSphere Client for vDS and vSS Configuration

To provision and manage a vDS, a vSphere Client must connect to a vCenter Server that manages the individual ESX hosts. The following conventions are used in the vSphere Client to provision and manage the virtual network:

Home → Inventory → Networking is the entry point for managing the virtual network across the datacenter and configuring a vDS.

- Provisioning vDS by selecting **datacenter** in left panel and then **new vNetwork Distributed Switch.** See Figure 8.
- Manage and configure a vDS by selecting the vDS name in left panel, then the **Configuration** tab in right panel. Add hosts to a vDS, configure and manage the DV Port Groups, dvUplinks and vDS properties through this panel. See Figure 9.

Figure 8 - Starting point in vSphere Client panel for creating vDS



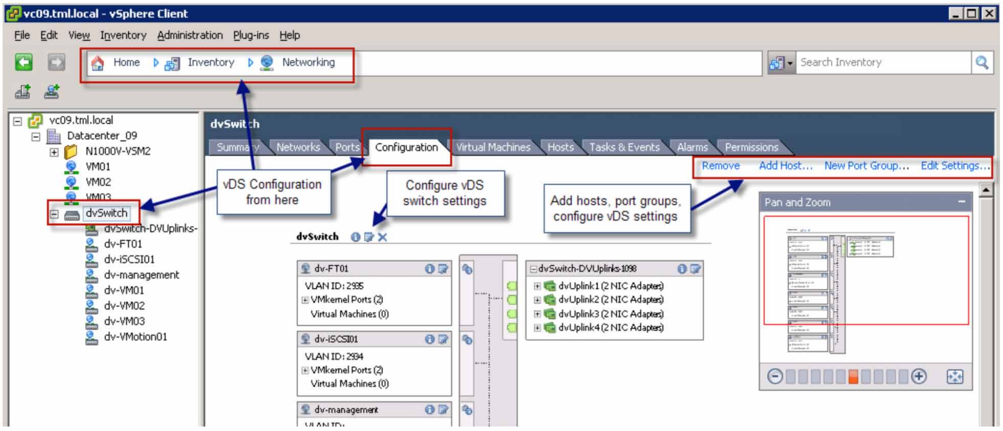
Networking Inventory selected

New vNetwork Distributed Switch

"Datacenter" level in hierarchy

Hosts: 4
Machines and Templates: 8
Clusters: 0
Networks: 20
Datastores: 8

Figure 9 - vSphere Client Panel for configuring vDS



vDS Configuration from here

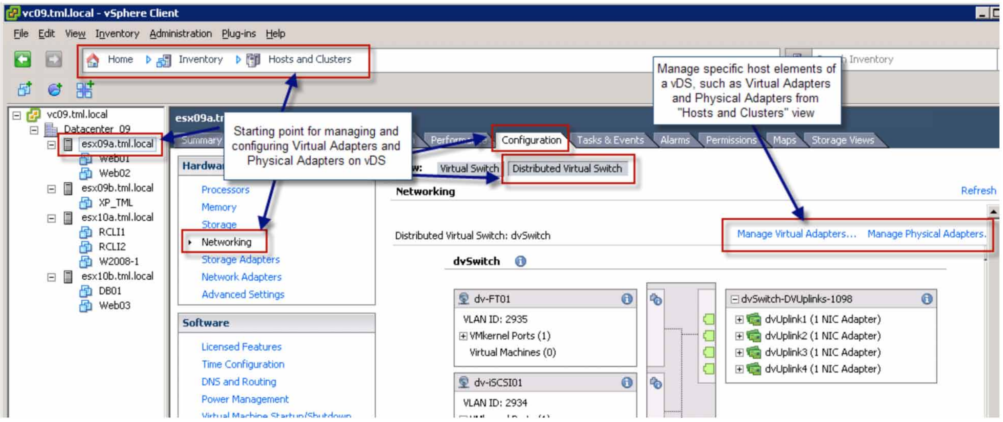
Configure vDS switch settings

Add hosts, port groups, configure vDS settings

Home > Inventory > Hosts and Clusters is the entry point for provisioning and managing the virtual network at the individual host level for a vSS and vDS. See Figure 10 below.

- Provision and manage all properties of a vSS by selecting a host in the left panel and the **Configuration** tab in right panel, then **Networking** in Hardware box. Select **Virtual Switch** under **View** at the top.
- Manage and configure the virtual adapters and physical adapters of a host with a provisioned vDS by selecting the host name in the left panel and the **Configuration** tab in right panel, then **Networking** in Hardware box. Select **Distributed Virtual Switch** under **View** at the top.

Figure 10 - vSphere Client panel for configuring vSS and specific host elements of a vDS



Starting point for managing and configuring Virtual Adapters and Physical Adapters on vDS

Manage specific host elements of a vDS, such as Virtual Adapters and Physical Adapters from "Hosts and Clusters" view

Home > Management > Host Profiles is the entry point to creating, editing, and applying Host Profiles.

Guided Example of Migration from a vNetwork Standard Switch to a vNetwork Distributed Switch

In this section, an example environment is used to illustrate the migration process from a vSS to a vDS. As mentioned in the first section of this document, multiple starting and ending configurations are possible. In this example, it's kept simple with a complete migration from a single vSS per host to a single vDS.

The example uses the two methods previously described, the vDS UI and Host Profiles, in migrating a four-host vSS environment to a vDS.

The example is organized as follows:

1. Create a vNetwork Distributed Switch (vDS)
2. Migration of resources from the Standard Switch to the vDS. i.e. vmnics, VMs using:
    - Per Host Manual Migration
    - Host Profiles

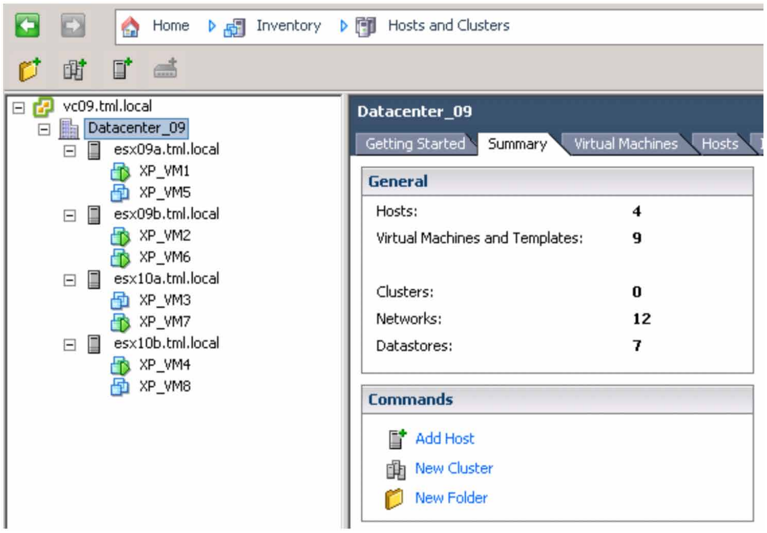
Configuration of Example Environment

The example environment shown in the following sections is comprised of the following:

1. Single vSphere Datacenter (Datacenter_09) on vCenter Server
2. Two ESX 4 Servers (esx09a.tml.local; esx10a.tml.local)
3. Two ESXi 4 Servers (esx09b.tml.local; esx10b.tml.local)
4. Eight Virtual Machines (Microsoft Windows XP) each with single vnic attachment to the vSwitch
5. Three VM networks (VM01; VM02; VM02)

The starting host inventory and virtual switch configuration from one of the ESX hosts is shown in Figure 11.

Figure 11 - Example Host Inventory from vSphere Client



- vc09.tml.local
    - Datacenter_09
        - esx09a.tml.local
            - XP_VM1
            - XP_VM5
        - esx09b.tml.local
            - XP_VM2
            - XP_VM6
        - esx10a.tml.local
            - XP_VM3
            - XP_VM7
        - esx10b.tml.local
            - XP_VM4
            - XP_VM8

Datacenter_09

General

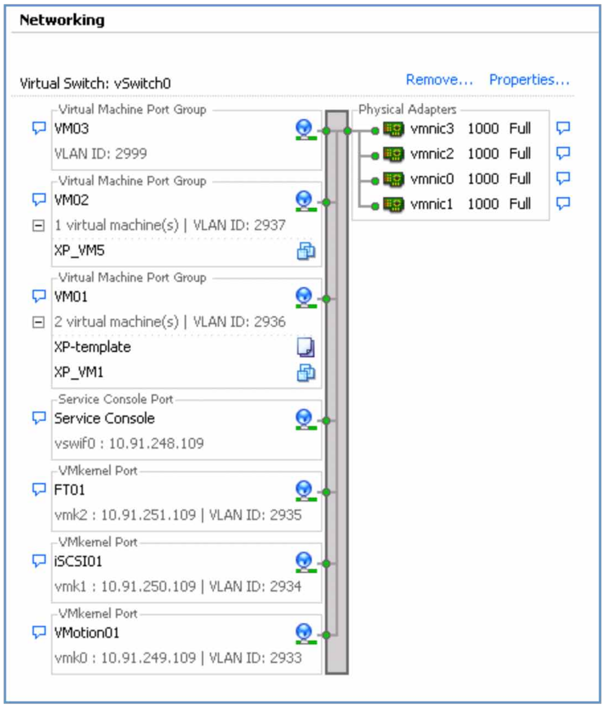
Hosts:	4
Virtual Machines and Templates:	9
Clusters:	0
Networks:	12
Datastores:	7

Each ESX and ESXi server is configured in the default environment with Port Groups on Standard Switches as follows:

1. Three Port Groups for Virtual Machines
    - VM01 – configured on VLAN 2936
    - VM02 – configured on VLAN 2937
    - VM03 – configured on VLAN 2999
2. Port Group for VMware® VMotion™
    - VMotion01 – configured on VLAN 2933
3. Port Group for iSCSI
    - iSCSI01 – configured on VLAN 2934
4. Port Group for VMware® Fault Tolerance (FT)
    - FT01 – configured on VLAN 2935

ESX Servers use the Service Console (SC) for management whereas ESXi Servers use a VMkernel port for management. The ESX servers (esx09a and esx10a) use a Service Console port configured on VLAN 1 (no VLAN listed in Port Group definition) and the ESXi servers (esx09b and esx10b) use a VMkernel port (vmk3) also configured on VLAN 1. (Note: Using VLAN 1 for management or any other purpose is not generally regarded as a networking best practice). Refer to Figure 12 and Figure 13 to see how the Port Groups are named and annotated for VLANs.

Figure 12 - Starting Example Standard Switch Configuration for ESX Server



Networking

Virtual Switch: vSwitch0

Virtual Machine Port Group
VM03
VLAN ID: 2999

Virtual Machine Port Group
VM02
1 virtual machine(s) | VLAN ID: 2937
XP_VM5

Virtual Machine Port Group
VM01
2 virtual machine(s) | VLAN ID: 2936
XP-template
XP_VM1

Service Console Port
Service Console
vswif0 : 10.91.248.109

VMkernel Port
FT01
vmk2 : 10.91.251.109 | VLAN ID: 2935

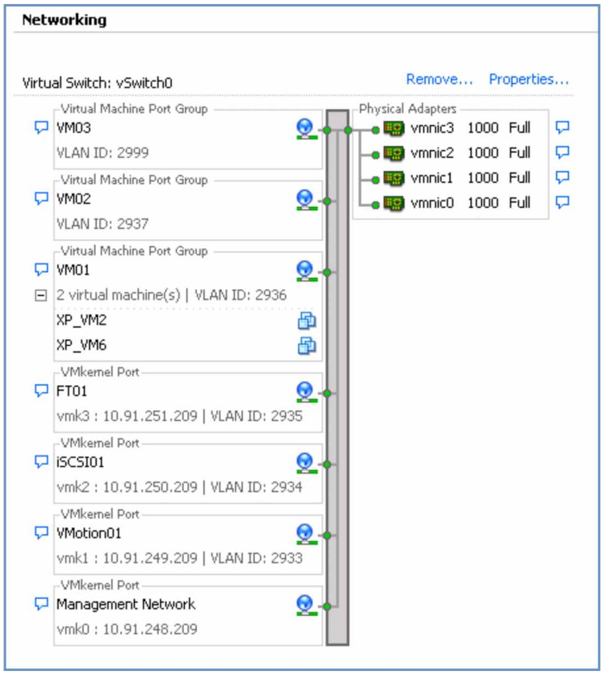
VMkernel Port
iSCSI01
vmk1 : 10.91.250.109 | VLAN ID: 2934

VMkernel Port
VMotion01
vmk0 : 10.91.249.109 | VLAN ID: 2933

Physical Adapters

vmnic3	1000	Full
vmnic2	1000	Full
vmnic0	1000	Full
vmnic1	1000	Full

Figure 13 - Starting Example Standard Switch Configuration for ESXi Server



Networking

Virtual Switch: vSwitch0

Virtual Machine Port Group
VM03
VLAN ID: 2999

Virtual Machine Port Group
VM02
VLAN ID: 2937

Virtual Machine Port Group
VM01
2 virtual machine(s) | VLAN ID: 2936
XP_VM2
XP_VM6

VMkernel Port
FT01
vmk3 : 10.91.251.209 | VLAN ID: 2935

VMkernel Port
iSCSI01
vmk2 : 10.91.250.209 | VLAN ID: 2934

VMkernel Port
VMotion01
vmk1 : 10.91.249.209 | VLAN ID: 2933

VMkernel Port
Management Network
vmk0 : 10.91.248.209

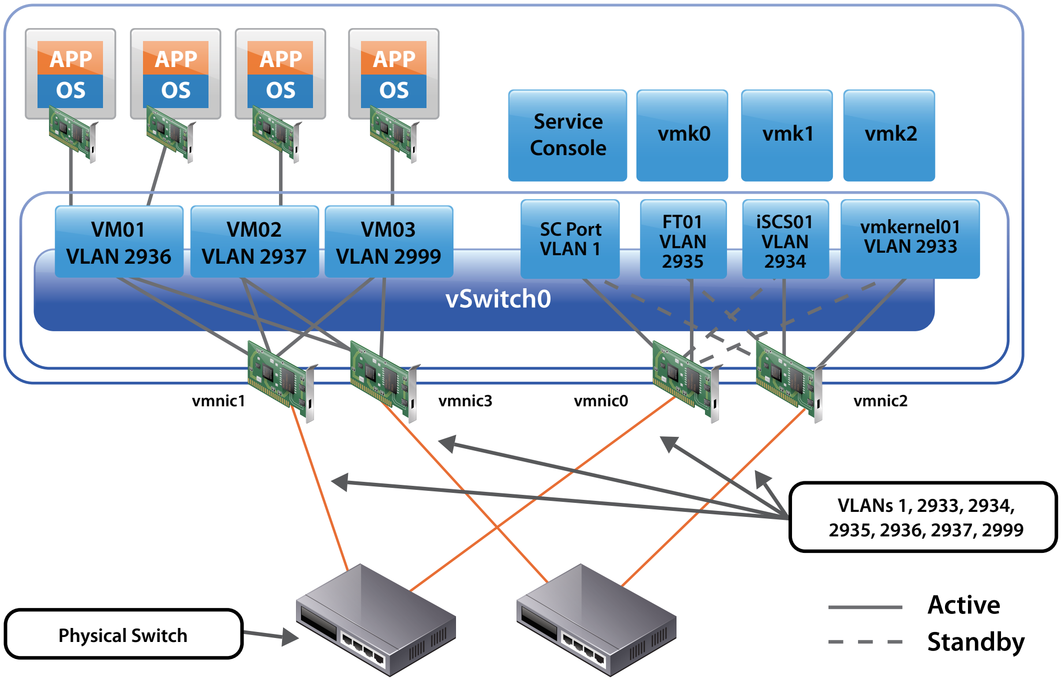
Physical Adapters

vmnic3	1000	Full
vmnic2	1000	Full
vmnic1	1000	Full
vmnic0	1000	Full

NIC Teaming Configuration

In the example server configuration, the original standard switch, Port Groups, and physical adapters are configured in a common and close to best practice design as shown in Figure 14.

Figure 14 - Example ESX Server showing NIC teaming configuration



1. All four vmnics are associated with a single vSS (vswitch0) with policy overrides on each of the Port Group definitions.
2. The Virtual Machine Port Groups (VM01, VM02, VM03) are configured to override the vSS settings and use:
   - Route Based on the Originating Virtual Port ID for the NIC Teaming load balancing policy
   - vmnic1 and vmnic3 as the Active Adapters (vmnic0 and vmnic2 are Unused Adapters).
3. The Service Console (or VMkernel management port on ESXi) and the FT01 Port Group are configured to:
   - Use Explicit failover order for the NIC Teaming Load Balancing policy
   - vmnic0 as the active adapter and vmnic2 as the standby adapter
4. The iSCSI01 and VMotion01 Port Groups are configured to:
   - Use Explicit failover order for the NIC Teaming Load Balancing policy
   - vmnic2 as the active adapter and vmnic0 as the standby adapter

You can see from the teaming configuration that each Port Group has two vmnics associated in either an Originating Virtual Port ID policy, or Explicit Failover Order. If one (and one only) vmnic was removed from each of these teams, connectivity would be maintained through the remaining vmnic.

VLAN Assignment

VLANs are assigned as shown in Table 2. These VLAN assignments, Port Group names, and Distributed Virtual Port Group names are used throughout the network section.

Table 2 – vSS Port Group to vDS DV Port Group mappings with corresponding VLAN numbering

Port Group name on vSS	Distributed Virtual Port Group name on vDS	VLAN
VM01	dv-VM01	2936
VM02	dv-VM02	2937
VM03	dv-VM03	2999
FT01	dv-FT01	2935
iSCSI01	dv-iSCSI01	2934
VMotion01	dv-VMotion01	2933
Management Network (ESXi) Service Console (ESX)	**dv-management**	**(native VLAN)**

Target Configuration

The target configuration is as follows:

- A single vDS spanning the four hosts (2x ESX 4; 2x ESXi 4)
- Distributed Virtual Port Groups spanning the four hosts with the same VLAN mapping as original environment (refer to Table 2).

Migrating to a vNetwork Distributed Switch

Two methods were described previously for migrating to a vNetwork Distributed Switch:

1. vDS UI only – This offers more per host control over migration, but is a longer process. Hosts do not need to be in maintenance mode so VMs can be powered up during migration.
2. vDS UI and Host Profiles –This uses a reference host template and is the recommended method for bulk vDS migration and deployment on hosts with inactive VMs. Host Profiles requires the target hosts to be in maintenance mode (i.e. VMs powered down).

These two methods are detailed in the following sections.

Method 1: Per Host vDS UI Migration to vDS

The objective in this part of the exercise is to completely migrate the current server environment running the standard switches to a vNetwork Distributed Switch. This migration includes all uplinks (also known as physical adapters, pnics, or vmnics), all Virtual Machine Port Groups, all VMkernel Ports, and Service Console Ports (for ESX Server).

Considerations for vDS Migration

Keep the following points in mind when migrating to a vDS:

1. Uplinks (physical nics or vmnics) can only be associated with one virtual switch (standard switch or vDS) at any one time. All four vmnics are migrated from the Standard Switch to the vDS in one step.

Note: If you must maintain VM connectivity (i.e. no outage) during migration, then you will need to migrate a subset of vmnics from the Standard Switch to the vDS so both switches have network connectivity. You will then have to migrate the virtual machines, and then finally, migrate the remaining vmnics. Note the intermediate step is critical for maintain VM connectivity.

2. You need to maintain a management connection to the server in order to perform any configuration tasks. (i.e. Service

Console on ESX server and the VMkernel Management Port on ESXi Server). Pay special attention to the management port in the migration.

3. If migrating a subset of vmnics rather than all at once, note the NIC teaming arrangement when selecting the vmnic migration order. The most critical is the SC or management port. If migrating an existing SC or management port, it must have a network path on the standard switch and also the vDS. Otherwise, you can risk losing connectivity with the ESX or ESXi Server after migration.

Creation and Migration Overview

The steps involved in a vDS UI migration of an existing environment using Standard Switches to a vDS are as follows:

1. Create vDS (without any associated hosts)
2. Create Distributed Virtual Port Groups on vDS to match existing or required environment
3. Add host to vDS and migrate vmnics to dvUplinks and Virtual Ports to DV Port Groups
4. Repeat Step 3 for remaining hosts

Creation and Migration Process

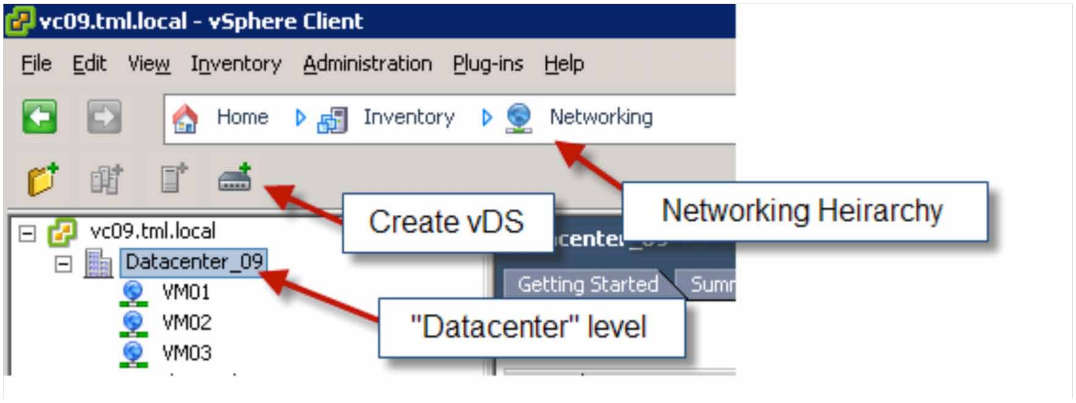
The following steps detail the migration of the 4-server example environment from standard switches to a single vNetwork Distributed Switch.

Note: Detailed step-by-step instructions for creating a vDS are shown in the ESX 4 Configuration Guide and ESXi 4 Configuration Guides available at http://www.vmware.com/support/pubs/.

Step 1: Create a vDS

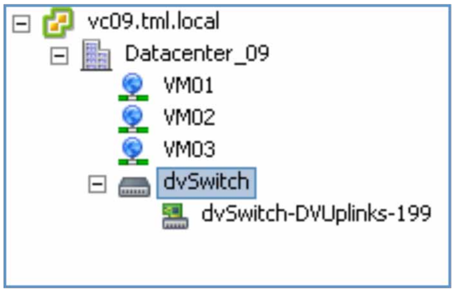
vNetwork Distributed Switches are created at the Datacenter level in the vSphere environment. A datacenter is the primary container for inventory objects such as hosts and virtual machines. The starting point is shown below from a vSphere Client attached to a vCenter Server. In the example environment, the Datacenter is labeled Datacenter_09.

Figure 15 - Starting point in vSphere Client for creating a vDS



After creating the vDS, the Networking Inventory panel will show a dvSwitch (the default name is chosen here), and an Uplink Group for the uplinks (in this example, this was named dvswitch-DVUplinks-199). Note that both these new items can be renamed to conform to any local naming standards.

Figure 16 -- Networking Inventory after creating a vDS



vc09.tml.local
Datacenter_09
VM01
VM02
VM03
dvSwitch
dvSwitch-DVUplinks-199

What is an Uplink Group?

An Uplink Group is a new feature with vDS. Much like a Port Group is a policy template for vnic attachment of VMs, VMkernel ports and service consoles, an Uplink Group is a policy template for the Uplinks on that vDS. Security policies, VLAN trunk ranges, traffic shaping and teaming/failover setting can set at this level for the entire vDS.

vDS uses dvUplinks to abstracts the actual physical vmnics on each host. NIC teaming with vDS uses the abstracted dvUplinks, so it's important the underlying physical vmnic distribution matches what is desired with attachment to the adjacent physical switches. In this environment, the same teaming arrangement is preserved meaning the vmnic to dvUplinks assignments must be chosen manually.

Step 2: Create Distributed Virtual Port Groups on vDS to Match Existing or Required Environment

In this step, a Distributed Virtual Port Groups on the vDS is created to match the existing environment and prepare the vDS for migration of the individual ports and Port Groups from the Standard Switches on each of the hosts.

What is a Distributed Virtual Port Group?

A Distributed Virtual Port Groups on a vDS is similar to a conventional Port Group on a Standard Switch except that can span multiple ESX and ESXi Servers. Port Groups and Distributed Virtual Port Groups are port templates that define port policies for similarly configured ports for attachment to VMs; VMkernel ports and Service Console ports.

Port Groups and Distributed Virtual Port Groups define:

- VLAN membership
- Port security policies (promiscuous mode, MAC address changes, Forged Transmits)
- Traffic shaping policies (egress from VM)
- NIC teaming policies for load balancing, failover detection and failback

In addition to these features and functions, a Distributed Virtual Port Group also defines:

- Ingress (to VM) traffic shaping policies (enabling bi-directional traffic shaping)
- Port Blocking policy

Port Group to DV Port Group Mappings

In this environment, the same VLAN structure and allocation is maintained as with the standard switch. To differentiate the DV Port Groups from the conventional Port Groups, they receive the prefix **dv.** Table 2 shows the mapping used for these port group names and corresponding VLAN associations.

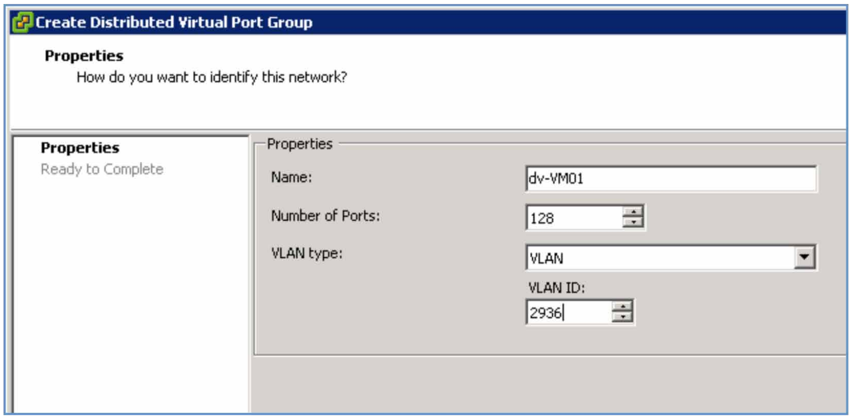
Note: In this example environment, the management traffic is untagged (meaning no VLAN tags) and as such uses the Native VLAN. By default with most physical switches, the Native VLAN is assigned to VLAN 1. Using the Native VLAN or VLAN 1 is not a best practice in many enterprises. A typical best practice network configuration would avoid use of VLAN 1 and the Native VLAN for all user and management traffic.

Creating the DV Port Groups

1. From the Network Inventory view, select the vDS. This is labeled dvSwitch in the example environment (see Figure 16). Then select **New Port Group**. This will bring up a **Create Distributed Virtual Port Group** panel.

   The first panel in creating the dv-VM01 DV Port Group is shown in Figure 17. Note the number of ports. This defaults to 128 and is the number of ports that this DV port group will allow once created. As this DV Port Group will support VMs, it means up to 128 VMs can use this DV Port Group. Modify this to a higher number if you need to support more VMs within a single DV Port Group. In this example environment, 128 ports are quite adequate.

Figure 17 - DV Port Group creation



Create Distributed Virtual Port Group

Properties
How do you want to identify this network?

Properties

Name: dv-VM01

Number of Ports: 128

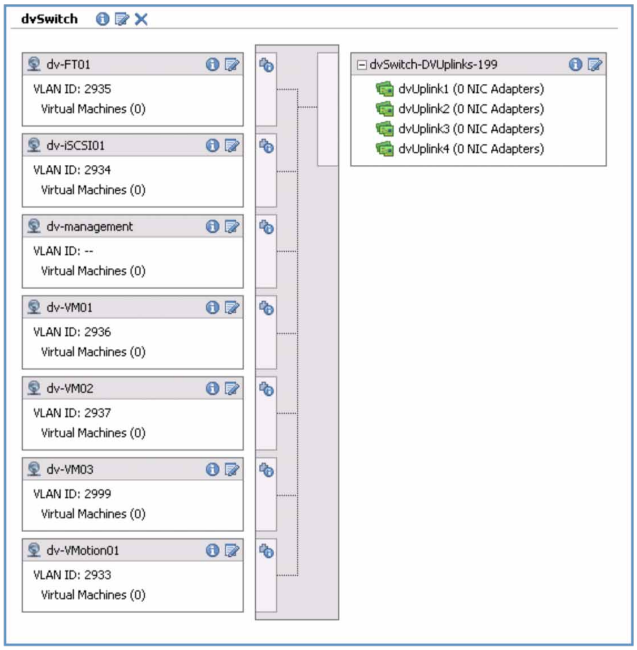
VLAN type: VLAN

VLAN ID: 2936

2. Continue creating the DV Port Groups according to the table. You will need to create DV Port Groups for each of the management and VMkernel ports as well (as shown in Table 2).

After creating the DV Port Groups, the vDS panel should look like Figure 18.

Figure 18 - vDS after creation of DV Port Groups



dvSwitch

dv-FT01
VLAN ID: 2935
Virtual Machines (0)

dv-iSCSI01
VLAN ID: 2934
Virtual Machines (0)

dv-management
VLAN ID: --
Virtual Machines (0)

dv-VM01
VLAN ID: 2936
Virtual Machines (0)

dv-VM02
VLAN ID: 2937
Virtual Machines (0)

dv-VM03
VLAN ID: 2999
Virtual Machines (0)

dv-VMotion01
VLAN ID: 2933
Virtual Machines (0)

dvSwitch-DVUplinks-199
dvUplink1 (0 NIC Adapters)
dvUplink2 (0 NIC Adapters)
dvUplink3 (0 NIC Adapters)
dvUplink4 (0 NIC Adapters)

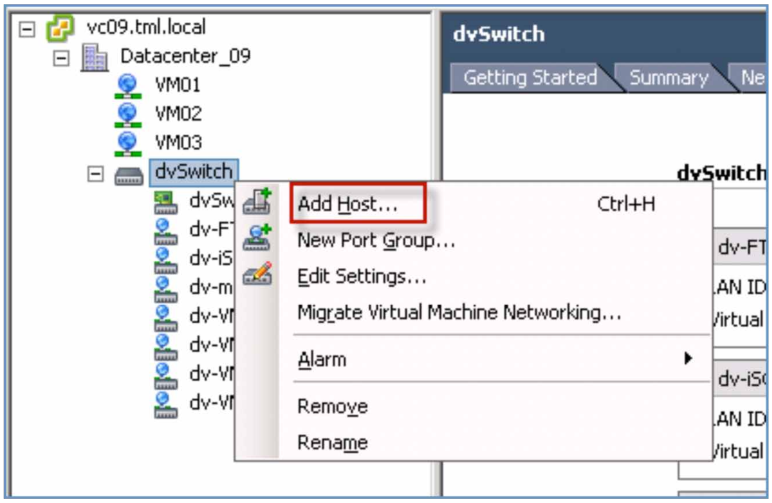
Step 3: Add host to vDS and migrate vmnics, Virtual Ports, and VM Networking

In this step, the Standard Switch environment of one host is migrated to the vDS and DV Port Groups created in steps 1 and 2. The process is described below.

Step 3a: Add Host to vDS

1. Switch to the **Home > Inventory > Networking** view
2. Right click on the vDS and select **Add Host**. This is shown in Figure 19.

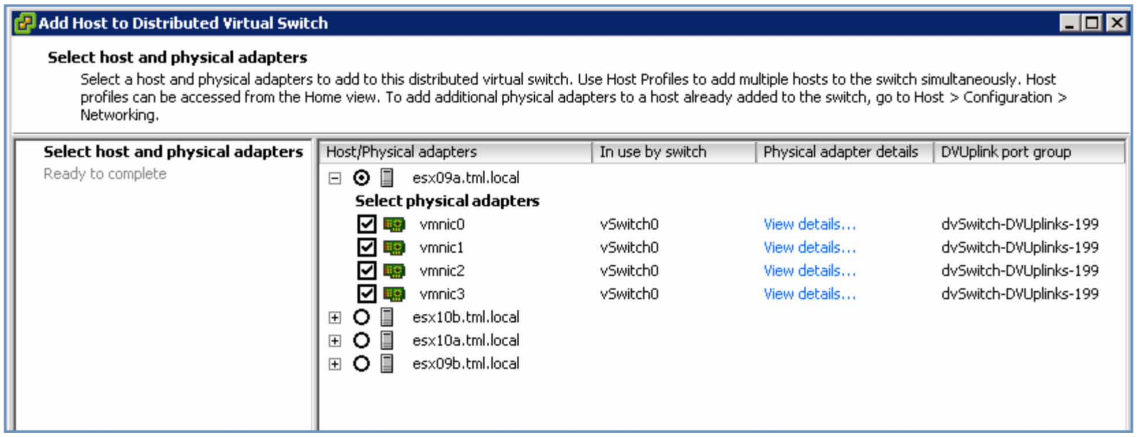
Figure 19 - Adding a host to a vDS



Step 3b: Select Physical Adapters (vmnics)

Next, select the host being migrated to vDS (esx09a.tml.local in this environment). For this example, all four vmnics are migrated from the Standard Switch on esx09a.tml.local to the vDS at one time. Refer to Figure 20.

Figure 20 - Selecting a host and vmnics for migration to vDS


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.

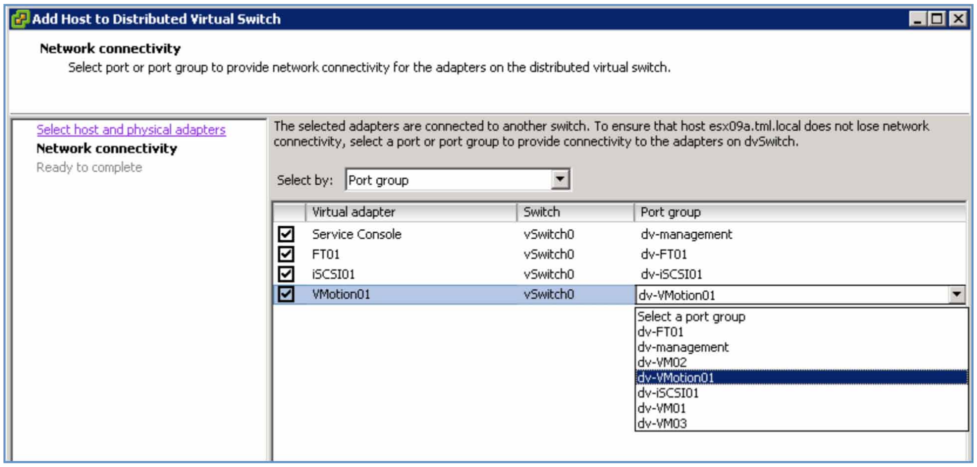
Select host and physical adapters
Ready to complete

Host/Physical adapters	In use by switch	Physical adapter details	DVUplink port group
⊟ ● esx09a.tml.local			
Select physical adapters			
☑ vmnic0	vSwitch0	View details...	dvSwitch-DVUplinks-199
☑ vmnic1	vSwitch0	View details...	dvSwitch-DVUplinks-199
☑ vmnic2	vSwitch0	View details...	dvSwitch-DVUplinks-199
☑ vmnic3	vSwitch0	View details...	dvSwitch-DVUplinks-199
⊞ ○ esx10b.tml.local			
⊞ ○ esx10a.tml.local			
⊞ ○ esx09b.tml.local			

Step 3c: Migrate Virtual Adapters

Now the virtual adapters on the Standard Switch with the DV Port Groups created in Step 2 need to be matched up. In this example, the Port Groups and DV Port Groups from Table 2 are matched up. Double check that the VLAN selected for the Management DV Port Group (dv-management in this example) matches that of the Service Console port (vswif0). Any mismatch or mistake with the service console definition could isolate the host and require ILO or console connection to restore connectivity. See Figure 21.

Figure 21 - Selecting Virtual Adapters for vDS migration



Add Host to Distributed Virtual Switch

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 esx09a.tml.local does not lose network connectivity, select a port or port group to provide connectivity to the adapters on dvSwitch.

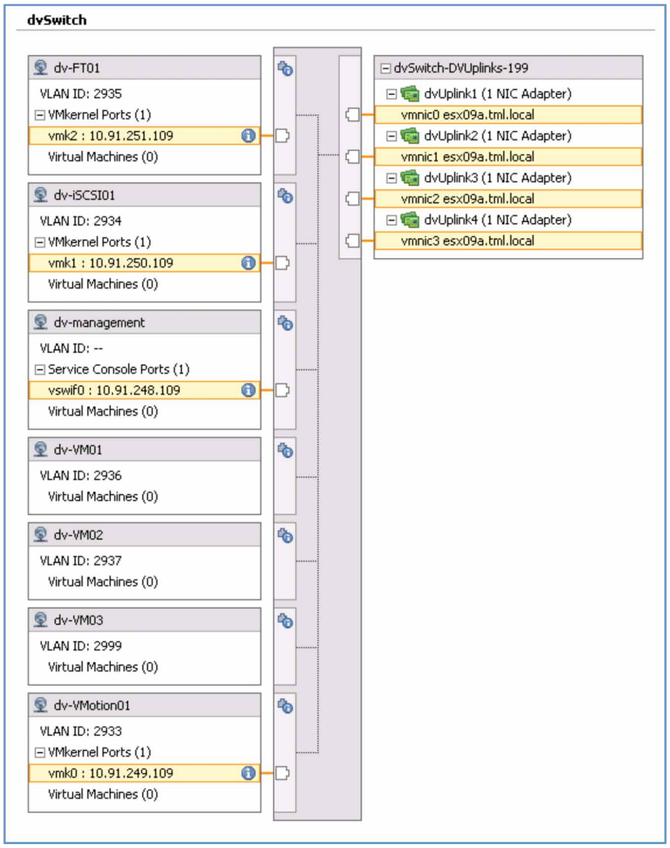
Select by: Port group

	Virtual adapter	Switch	Port group
☑	Service Console	vSwitch0	dv-management
☑	FT01	vSwitch0	dv-FT01
☑	iSCSI01	vSwitch0	dv-iSCSI01
☑	VMotion01	vSwitch0	dv-VMotion01

The vSphere Client will then present a preview of the changes to the vDS prior to actual executing them. These are shown as highlights on a vDS panel. See Figure 22. Double check the changes once again, particularly the management port (Service Console for ESX or VMkernel port for ESXi).

Once checked, click on the **Finish** button and wait for the operation to complete. You can track the status in the Recent Tasks panel at the bottom of the vSphere Client panel. Note that the operation may take around a minute to complete. Note that this step does not transfer the Port Groups for the VMs — they are still associated with the Standard Switch. As all the vmnics are removed from the Standard Switch, these VMs will be disconnected from the network.

Figure 22 - Preview of changes to vDS prior to actual migration step



dvSwitch

dv-FT01
VLAN ID: 2935
VMkernel Ports (1)
vmk2 : 10.91.251.109
Virtual Machines (0)

dv-iSCSI01
VLAN ID: 2934
VMkernel Ports (1)
vmk1 : 10.91.250.109
Virtual Machines (0)

dv-management
VLAN ID: --
Service Console Ports (1)
vswif0 : 10.91.248.109
Virtual Machines (0)

dv-VM01
VLAN ID: 2936
Virtual Machines (0)

dv-VM02
VLAN ID: 2937
Virtual Machines (0)

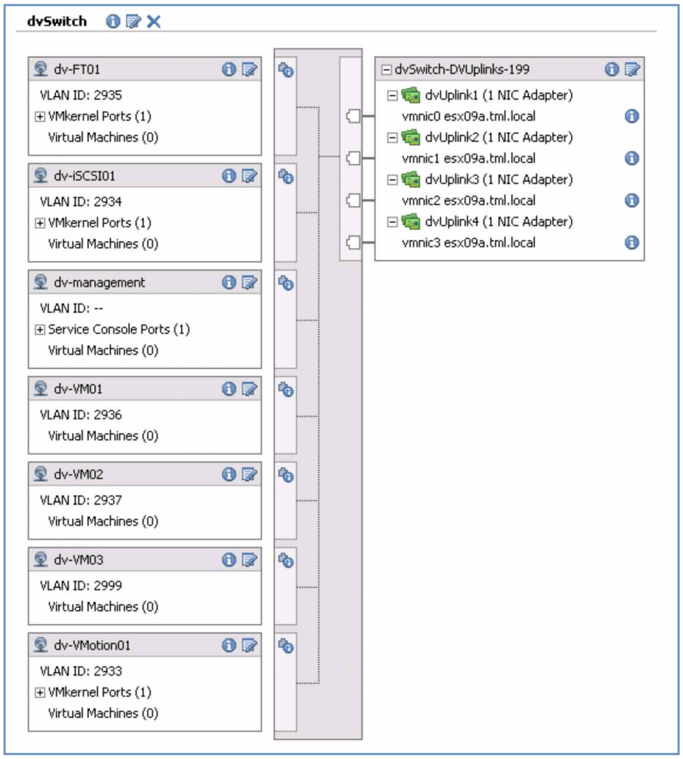
dv-VM03
VLAN ID: 2999
Virtual Machines (0)

dv-VMotion01
VLAN ID: 2933
VMkernel Ports (1)
vmk0 : 10.91.249.109
Virtual Machines (0)

dvSwitch-DVUplinks-199
dvUplink1 (1 NIC Adapter)
vmnic0 esx09a.tml.local
dvUplink2 (1 NIC Adapter)
vmnic1 esx09a.tml.local
dvUplink3 (1 NIC Adapter)
vmnic2 esx09a.tml.local
dvUplink4 (1 NIC Adapter)
vmnic3 esx09a.tml.local

The vDS should now appear as in Figure 23. All of the Standard Switch Environment, except for the VMs, should now be transferred to the vDS.

Figure 23 - vDS after migration of one host



dvSwitch

dv-FT01
VLAN ID: 2935
⊞ VMkernel Ports (1)
Virtual Machines (0)

dv-iSCSI01
VLAN ID: 2934
⊞ VMkernel Ports (1)
Virtual Machines (0)

dv-management
VLAN ID: --
⊞ Service Console Ports (1)
Virtual Machines (0)

dv-VM01
VLAN ID: 2936
Virtual Machines (0)

dv-VM02
VLAN ID: 2937
Virtual Machines (0)

dv-VM03
VLAN ID: 2999
Virtual Machines (0)

dv-VMotion01
VLAN ID: 2933
⊞ VMkernel Ports (1)
Virtual Machines (0)

⊟ dvSwitch-DVUplinks-199
⊟ dvUplink1 (1 NIC Adapter)
vmnic0 esx09a.tml.local
⊟ dvUplink2 (1 NIC Adapter)
vmnic1 esx09a.tml.local
⊟ dvUplink3 (1 NIC Adapter)
vmnic2 esx09a.tml.local
⊟ dvUplink4 (1 NIC Adapter)
vmnic3 esx09a.tml.local

Step 3d: Migrate Virtual Machine Networking

Now the VMs can be migrated to the vDS. (The VMs on Port Groups VM01, VM02, and VM03 in this environment). Note that if you are migrating a number of hosts to a vDS, you can optionally leave this until last as you can migrate all Virtual Machine Networking for all hosts on the vDS at once.

To begin the process:

1. Right-click on the vDS from **Home > Inventory > Networking** panel and select **Migrate Virtual Machine Networking** from the list (see Figure 24).
2. Select the source network from the standard switch and the destination network on the vDS. In this example, the VM01 is migrated to dv-VM01. Refer to Figure 25.
3. Click on **Show Virtual Machines**. This will present a list of eligible VMs on the source network on the migrated host (or hosts).
4. Select the VMs you wish to migrate (all of them in this case).
5. Repeat for each of the remaining VM networking Port Groups.

Figure 24 - Migrating Virtual Machine Networking to vDS

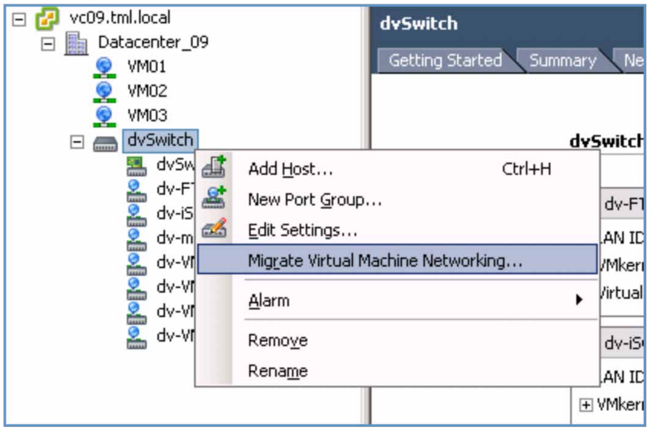
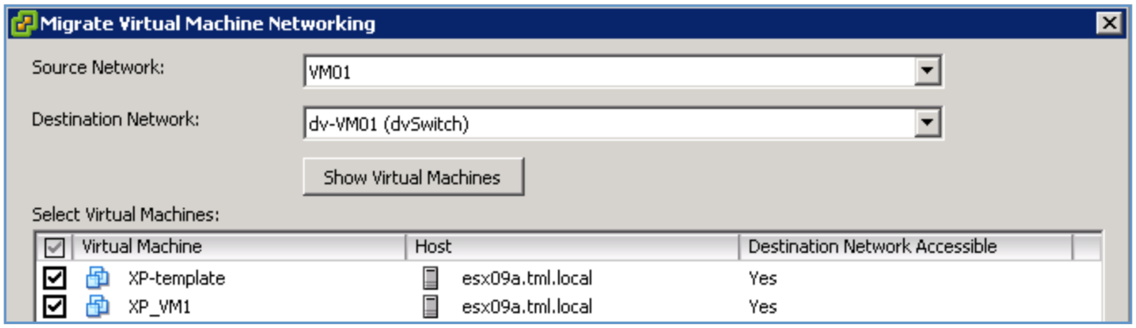


Figure 25 - Migrating VM Networking — selecting VMs



Source Network: VM01

Destination Network: dv-VM01 (dvSwitch)

Select Virtual Machines:

☑	Virtual Machine	Host	Destination Network Accessible
☑	XP-template	esx09a.tml.local	Yes
☑	XP_VM1	esx09a.tml.local	Yes

Step 4: Repeat Step 3 for Remaining Hosts

Step 3 migrated the Standard Switch environment to a vDS for one host. Repeat this step to migrate more hosts to a vDS.

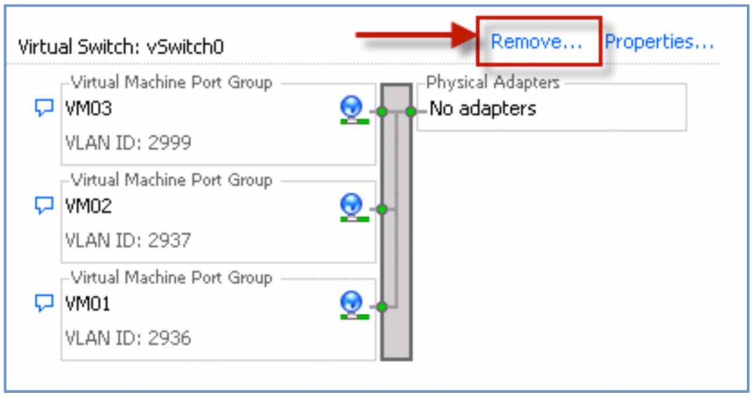
Step 5: Optionally Delete Standard Switches from Hosts

If you decided to migrate all virtual networking to vDS, you can now delete the Standard Switches from each migrated host.

To delete the Standard Switch (vSwitch0), do the following:

1. Go to the **Home > Inventory > Hosts** and Clusters view and select the **Configuration** tab and then **Networking** from the Hardware box.
2. Select **Remove** from the panel above the vSwitch0 graphic (Refer to Figure 26).

Figure 26 - Removing a Standard Switch



Step 6: Adjusting Distributed Virtual Port Groups Policies

When creating the DV Port Groups earlier, this example only configured the VLAN number and did not configure the NIC teaming policies. Each of the DV Port Groups is using the default NIC teaming assignments of Originating Virtual Port load balancing over all four dvUplinks. If you wish to restore the NIC teaming policies used prior to the vDS migration (shown in Figure 14), edit each of the DV Port Group configurations.

Table 3 details the policies used in the example environment. These are the same policies used with the Standard Switches. See Figure 14 for graphic representation of NIC teaming assignments.

The policies are selected in this manner to maintain availability upon any single point of failure from the physical network. Vmnic0 and vmnic1 are connected to one adjacent physical switch (Switch#1); vmnic2 and vmnic3 are connected to another adjacent physical switch (switch#2). If either physical switch fails, the load balancing and failover policies will ensure each of the ports supported by the DV Port Groups will continue operation.

Table 3 - DV Port Group Load Balancing Policies

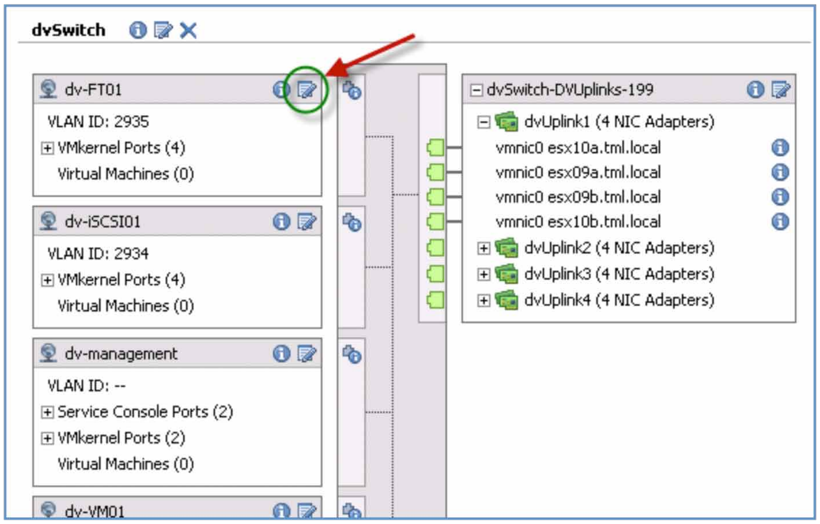
DV Port Group	VLAN	Load Balancing	dvUplink1 (vmnic0) Switch#1	dvUplink2 (vmnic1) Switch#1	dvUplink3 (vmnic2) Switch#2	dvUplink4 (vmnic3) Switch#2
dv-VM01	2936	Orig Virtual Port	Unused	**Active**	Unused	**Active**
dv-VM02	2937	Orig Virtual Port	Unused	**Active**	Unused	**Active**
dv-VM03	2999	Orig Virtual Port	Unused	**Active**	Unused	**Active**
dv-FT01	2935	Explicit Failover	**Active**	Unused	Standby	Unused
dv-iSCSI01	2934	Explicit Failover	Standby	Unused	**Active**	Unused
dv-VMotion01	2933	Explicit Failover	Standby	Unused	**Active**	Unused
dv-management	native	Explicit Failover	**Active**	Unused	Standby	Unused

Editing DV Port Group Policies

From the Networking Inventory view of the vDS, select the **notepad and pen** icon from each DV Port Group to edit the policy settings. This icon is shown in Figure 27.

Select the **Teaming and Failover** panel to adjust the Load Balancing and failover order of the links according to the policies shown in Table 3.

Figure 27 - Editing DV Port Group Policies



How vDS Helps with Policy Adjustments

Because the vDS and DV Port Groups are used, this last stage of adjusting the load balancing and failover policies required a single edit for each port group needing to be changed. All hosts covered by the vDS were automatically updated with the new policies. (i.e. the changes were independent of the number of hosts.) Without vDS and using a standard switch environment (as in VI3), the Port Groups on each and every host would need to be edited.

In the four host example environment, this means just eight changes for eight DV Port Groups with vDS versus 32 changes (4x8) for the corresponding Standard Switch environment.

The vDS is now ready for migration.

Summary of vDS UI Migration Method

The process outlined above makes it easy to migrate individual or small numbers of hosts to a vDS. It also avoids the need for putting any hosts in Maintenance Mode. Note that Host Profiles provide a simple way to migrate a large number of hosts in one step. The Host Profile method is described in the next section of this document.

Method 2: vDS Migration using Host Profiles

In this section, you'll learn how to deploy a vNetwork Distributed Switch (vDS) using Host Profiles. Host Profiles is the recommended method for deploying a vDS over a large population of similarly configured hosts.

Considerations for using Host Profiles for Deploying vDS

Note the following when using Host Profiles for deploying a vDS:

- Target hosts must be in Maintenance Mode. This means all VMs must be powered off or migrated to other hosts. If this is a problem, consider a phased deployment or use the per host vDS UI migration method described earlier.
- An ESX Host Profile can be applied to ESX and ESXi hosts. An ESXi Host Profile can only be applied to an ESXi Host. If you have a mix of ESX and ESXi hosts, then create the Host Profile from an ESX host. The Host Profile feature in vCenter Server is able to translate and apply the ESX Service Console definition to an ESXi VMkernel port for management access.

Process Overview

For this example, the following procedure to migrate the example environment to vDS is used. The starting point is four hosts, each with a single Standard Switch (formerly known as a vSwitch).

The first four steps are the same as the per host manual migration method described prior. At the completion of Step 4, a single host with its networking environment completely migrated to vDS will be created.

1. Create vDS (without any associated hosts)
2. Create Distributed Virtual Port Groups on vDS to match existing or required environment
3. Add host to vDS and migrate vmnics to dvUplinks and Virtual Ports to DV Port Groups
4. Delete Standard Switch from host

The next three steps apply only when using host profiles. They allow us to create a profile of this migrated host and then apply it to a number of hosts in one step (Step 7).

5. Create Host Profile of Reference Host
6. Attach and apply host profile to candidate hosts
7. Migrate VM networking for VMs and take hosts out of Maintenance Mode.

It may seem more steps are involved in using Host Profiles versus the Per Host Manual Method described earlier. However, since the Host Profile applies to multiple hosts, the steps above are independent of the number of hosts.

Step 1 to Step 4: Migrate Reference Host to vDS

Select a host to be used as a **Reference Host**. If you wish to apply the Host Profile over a mixed ESX and ESXi environment, then the reference host must be an ESX host.

Follow Steps 1 to 4 of the Per Host vDS UI Migration method described earlier.

At completion of Step 4, you should have a single reference host with its virtual networking environment entirely migrated to a VDS.

With this example environment, ***esx09a.tml.local*** is the Reference Host.

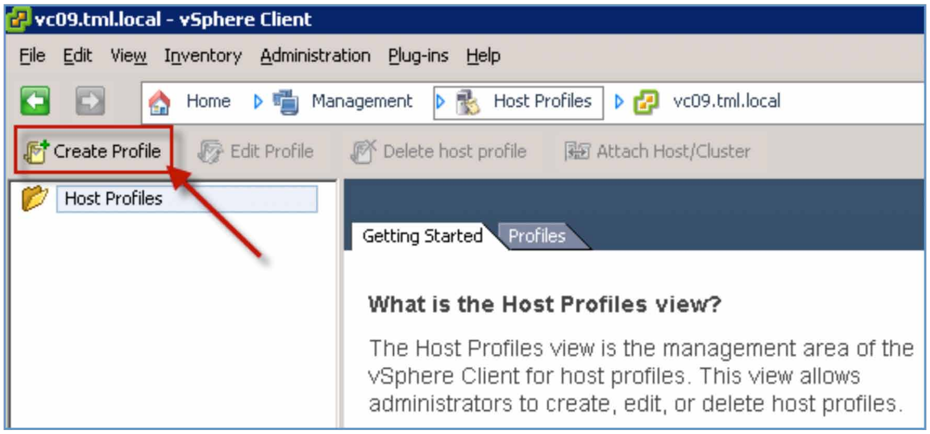
Step 5: Create Host Profile of Reference Host

With the vDS looking like the example in Figure 23, a Host Profile of this host (esx09a) was created and then applied across the other hosts the cluster.

Follow the following steps to create a Host Profile from the example reference host:

1. Go to the **Home > Management > Host Profiles** view in the vSphere Client
2. Select **Create Profile** (see Figure 28)

Figure 28 - Host Profiles Panel

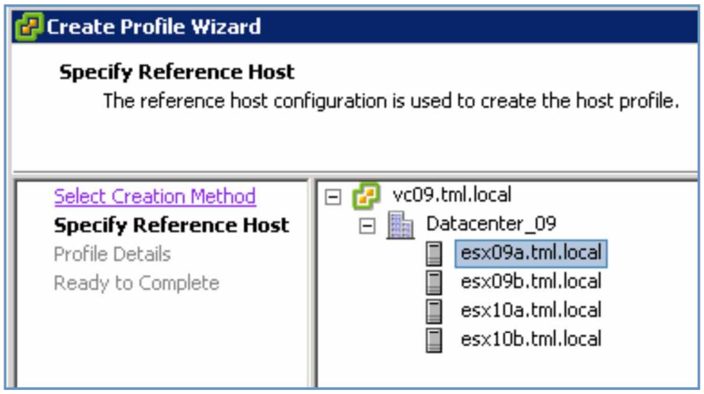


What is the Host Profiles view?

The Host Profiles view is the management area of the vSphere Client for host profiles. This view allows administrators to create, edit, or delete host profiles.

3. Select **Create Profile** from existing host
4. Select the desired Reference Host in the Create Profile UI (see Figure 29)

Figure 29 - Specifying Reference Host for Host Profile



Specify Reference Host

The reference host configuration is used to create the host profile.

5. Create a meaningful name (i.e. "esx09a-vDS profile") and description for the Host Profile and click **Next** and then **Finish**. After execution, a Host Profile will appear in the left panel.

6. At this point, you can edit, delete, or attach the host profile to a host or cluster. The edit capability allows fine-tuning of the profile to add or remove components or change settings.

Step 6: Attach and Apply Host Profile to Candidate Hosts

Host Profiles can only be applied to hosts in Maintenance Mode. All VMs are powered down in Maintenance Mode. If you have powered up VMs, either shut them down or migrate them to another host.

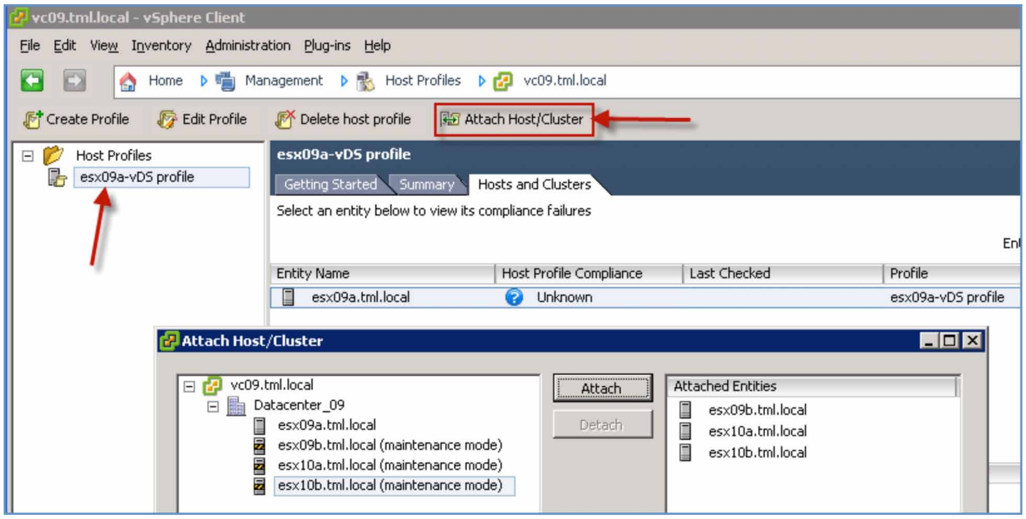
When the Host Profile is applied to each of the hosts, a dialog box will ask for the IP address of each of the virtual adapters that will be migrated with the host profile. To prepare for this, gather the IP addresses for the virtual adapters on each of the hosts. The IP addresses for this example environment are shown in Table 4.

Table 4 - IP Addresses of Virtual Adapters in example environment

Host	Management	iSCSI01	VMotion01	FT01
esx09a (ESX)	10.91.248.109	10.91.250.109	10.91.249.109	10.91.251.109
esx09b (ESXi)	10.91.248.209	10.91.250.209	10.91.249.209	10.91.251.209
esx10a (ESX)	10.91.249.110	10.91.250.110	10.91.249.110	10.91.251.110
esx10b (ESXi)	10.91.248.210	10.91.250.210	10.91.249.210	10.91.251.210

1. Put the hosts in Maintenance Mode. From the **Hosts > Inventory > Hosts and Clusters** panel, right-click on each host and select **Enter Maintenance Mode**. Select **Yes** in the confirmation dialog box.
2. Return to the **Home > Management > Host Profiles** panel, select the profile created in Step 5 above and click **Attach Host/ Cluster** (see Figure 30).
3. An Attach Host/Cluster is where you can select which hosts to attach to the selected host profile. Click **Attach** for each of the hosts to which you will apply the host profile and click **OK**. Note: The profile is not yet committed to the hosts, so there is still time to back out.

Figure 30 - Attaching a Host/Cluster to Host Profile

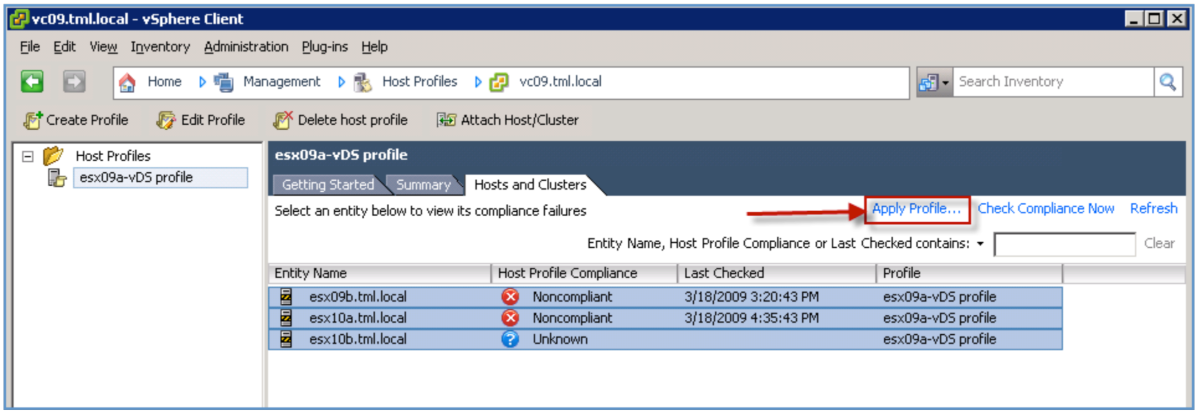

vc09.tml.local - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Management Host Profiles vc09.tml.local
Create Profile
Edit Profile
Delete host profile
Attach Host/Cluster
Host Profiles
esx09a-vDS profile
esx09a-vDS profile
Getting Started
Summary
Hosts and Clusters
Select an entity below to view its compliance failures
Ent
Attach Host/Cluster
vc09.tml.local
Datacenter_09
esx09a.tml.local
esx09b.tml.local (maintenance mode)
esx10a.tml.local (maintenance mode)
esx10b.tml.local (maintenance mode)
Attach
Detach

Entity Name	Host Profile Compliance	Last Checked	Profile
esx09a.tml.local	Unknown		esx09a-vDS profile

Attached Entities
esx09b.tml.local
esx10a.tml.local
esx10b.tml.local

4. At this point, you can apply the Host Profile to one or more hosts from the Host Profiles panel by control-click each host and then clicking on **Apply Profile**.

Figure 31 - Selecting Hosts to which to apply a Host Profile



vc09.tml.local - vSphere Client

esx09a-vDS profile

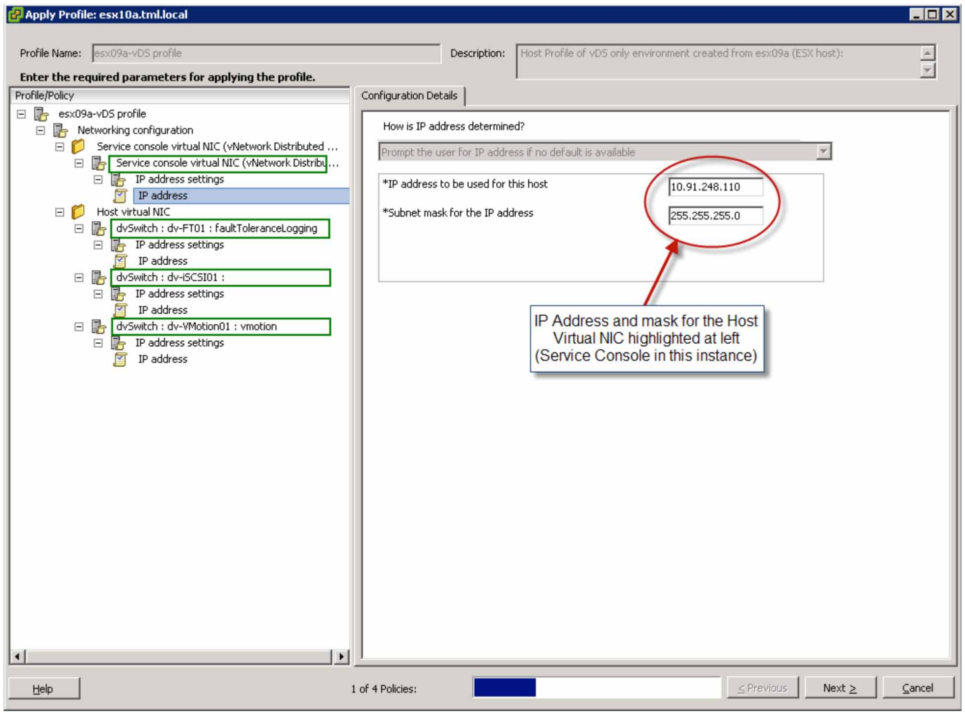
Select an entity below to view its compliance failures

Entity Name, Host Profile Compliance or Last Checked contains:

Entity Name	Host Profile Compliance	Last Checked	Profile
esx09b.tml.local	Noncompliant	3/18/2009 3:20:43 PM	esx09a-vDS profile
esx10a.tml.local	Noncompliant	3/18/2009 4:35:43 PM	esx09a-vDS profile
esx10b.tml.local	Unknown		esx09a-vDS profile

5. This will bring up the panel shown in Figure 32. Insert the IP addresses and masks as prompted for each host. For this example, the address used in Table 4 was used.

Figure 32 - Filling in IP Address details for Host Virtual NICs as the host profile is applied to a host



Apply Profile: esx10a.tml.local

Profile Name: esx09a-vDS profile

Description: Host Profile of vDS only environment created from esx09a (ESX host):

Enter the required parameters for applying the profile.

How is IP address determined?

Prompt the user for IP address if no default is available

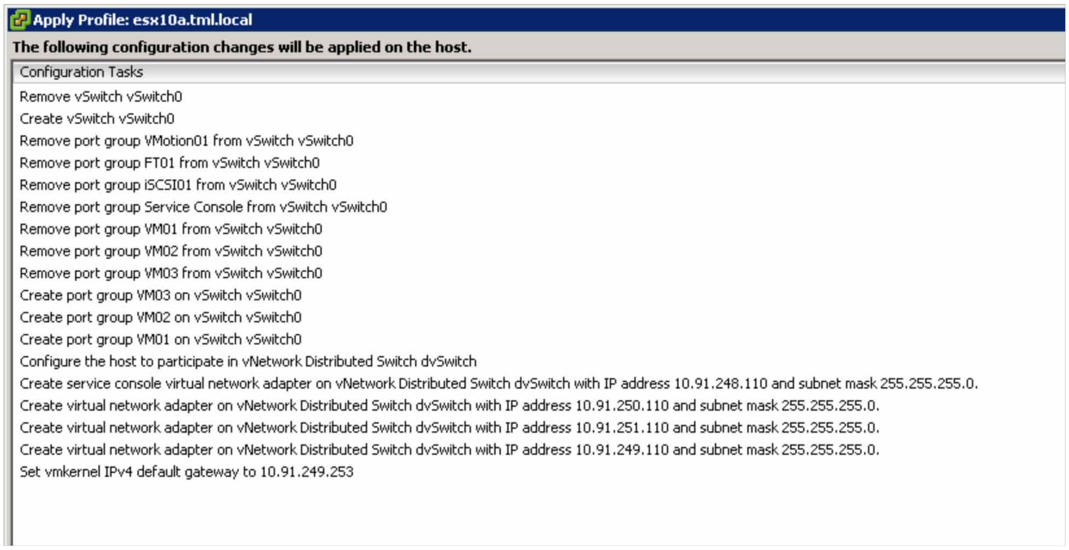
*IP address to be used for this host: 10.91.248.110

*Subnet mask for the IP address: 255.255.255.0

IP Address and mask for the Host Virtual NIC highlighted at left (Service Console in this instance)

6. When **Next** is selected, a panel will appear indicating what changes will be made by the host profile. Figure 33 shows what will happen when the host profile is applied to esx10b (ESXi host).

Figure 33 - Report of what the Host Profile will change once applied to the host.



The following configuration changes will be applied on the host.

Configuration Tasks

```
Remove vSwitch vSwitch0
Create vSwitch vSwitch0
Remove port group VMotion01 from vSwitch vSwitch0
Remove port group FT01 from vSwitch vSwitch0
Remove port group iSCSI01 from vSwitch vSwitch0
Remove port group Service Console from vSwitch vSwitch0
Remove port group VM01 from vSwitch vSwitch0
Remove port group VM02 from vSwitch vSwitch0
Remove port group VM03 from vSwitch vSwitch0
Create port group VM03 on vSwitch vSwitch0
Create port group VM02 on vSwitch vSwitch0
Create port group VM01 on vSwitch vSwitch0
Configure the host to participate in vNetwork Distributed Switch dvSwitch
Create service console virtual network adapter on vNetwork Distributed Switch dvSwitch with IP address 10.91.248.110 and subnet mask 255.255.255.0.
Create virtual network adapter on vNetwork Distributed Switch dvSwitch with IP address 10.91.250.110 and subnet mask 255.255.255.0.
Create virtual network adapter on vNetwork Distributed Switch dvSwitch with IP address 10.91.251.110 and subnet mask 255.255.255.0.
Create virtual network adapter on vNetwork Distributed Switch dvSwitch with IP address 10.91.249.110 and subnet mask 255.255.255.0.
Set vmkernel IPv4 default gateway to 10.91.249.253
```

Step 7: Migrate VM Networking to vDS

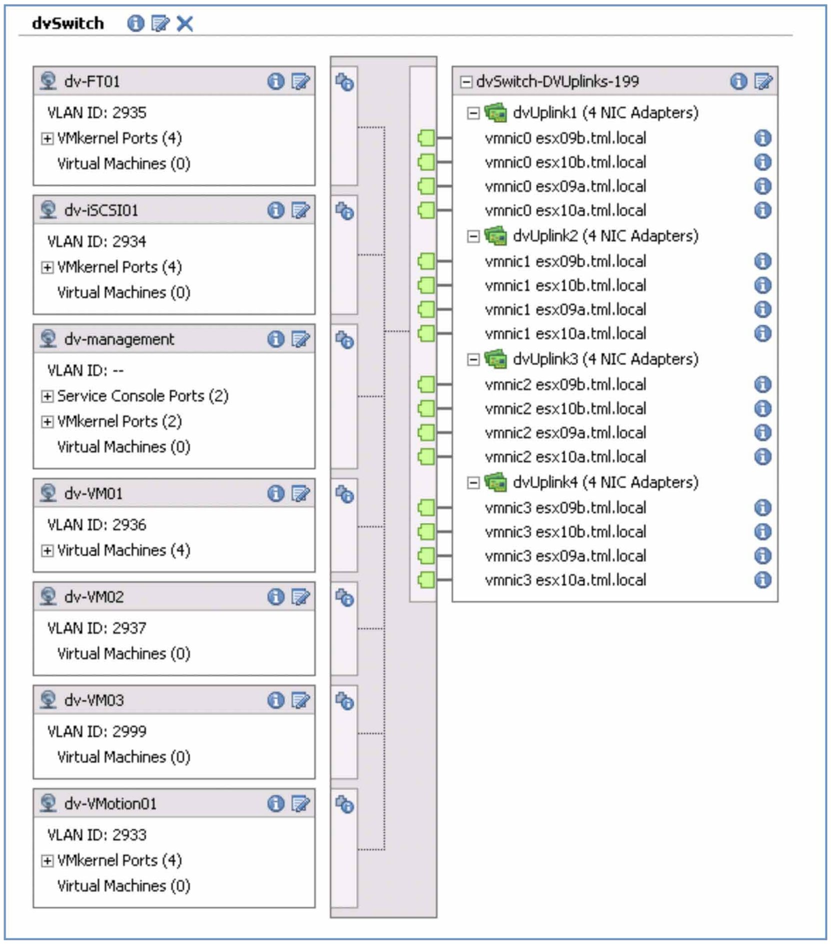
Next, this example migrates the VMs from the vSS Port Groups to the vDS DV Port Groups using the same method described earlier with the vDS UI in the section titled: Step3d: Migrate Virtual Machine Networking.

Go to the **Home > Inventory > Networking** panel and right click on the vDS and select **Migrate Virtual Machine Networking**. Select the appropriate Source Networks (vSS Port Groups) and Destination Networks (vDS DV Port Groups) to perform the migration.

vDS After Migration

After using either of the methods (Per host manual method or Host Profile method) described above, the vDS should appear as shown in Figure 34.

Figure 34 - vDS after complete migration of all ports and uplinks in example environment



dvSwitch

dv-FT01
VLAN ID: 2935
⊞ VMkernel Ports (4)
Virtual Machines (0)

dv-iSCSI01
VLAN ID: 2934
⊞ VMkernel Ports (4)
Virtual Machines (0)

dv-management
VLAN ID: --
⊞ Service Console Ports (2)
⊞ VMkernel Ports (2)
Virtual Machines (0)

dv-VM01
VLAN ID: 2936
⊞ Virtual Machines (4)

dv-VM02
VLAN ID: 2937
Virtual Machines (0)

dv-VM03
VLAN ID: 2999
Virtual Machines (0)

dv-VMotion01
VLAN ID: 2933
⊞ VMkernel Ports (4)
Virtual Machines (0)

⊟ dvSwitch-DVUplinks-199
⊟ dvUplink1 (4 NIC Adapters)
vmnic0 esx09b.tml.local
vmnic0 esx10b.tml.local
vmnic0 esx09a.tml.local
vmnic0 esx10a.tml.local
⊟ dvUplink2 (4 NIC Adapters)
vmnic1 esx09b.tml.local
vmnic1 esx10b.tml.local
vmnic1 esx09a.tml.local
vmnic1 esx10a.tml.local
⊟ dvUplink3 (4 NIC Adapters)
vmnic2 esx09b.tml.local
vmnic2 esx10b.tml.local
vmnic2 esx09a.tml.local
vmnic2 esx10a.tml.local
⊟ dvUplink4 (4 NIC Adapters)
vmnic3 esx09b.tml.local
vmnic3 esx10b.tml.local
vmnic3 esx09a.tml.local
vmnic3 esx10a.tml.local

vDS Usage Examples

Now a vDS is configured across four hosts, it's time to take a closer look at its capabilities.

The vNetwork Distributed Switch simplifies virtual network administration particularly across a large number of hosts. As described previously, simple changes to port groups that would formerly require the same change across all hosts to keep consistency (when using VMotion, for example), now only require a single change to a distributed port group.

To illustrate this, this example shows what occurs when the VLAN assignment for a set of VMs is changing. (i.e. changing the VLAN for all the VMs using VLAN 2999 to VLAN 2995). The approach to changing this for a Standard Switch versus a vDS is as follows:

Changes using the Standard Switch

In this example environment, VM03 was used as the Port Group for all VMs on VLAN 2999. To change to VLAN 2995, and ensure VMotion would continue to work without issue, you would need to change the Port Group on each and every host.

This is not a difficult exercise in this sample four-host environment, although it does require four separate changes — one for each host. In an environment with 50 hosts, for example, the burden of 50 individual changes becomes much more significant, time consuming and raises the likelihood of human error.

Changes using the vNetwork Distributed Switch

The per host change burden goes away when using a vDS with a Distributed Port Group. A single change to the Distributed Virtual Port Group applies to all hosts using that vDS.

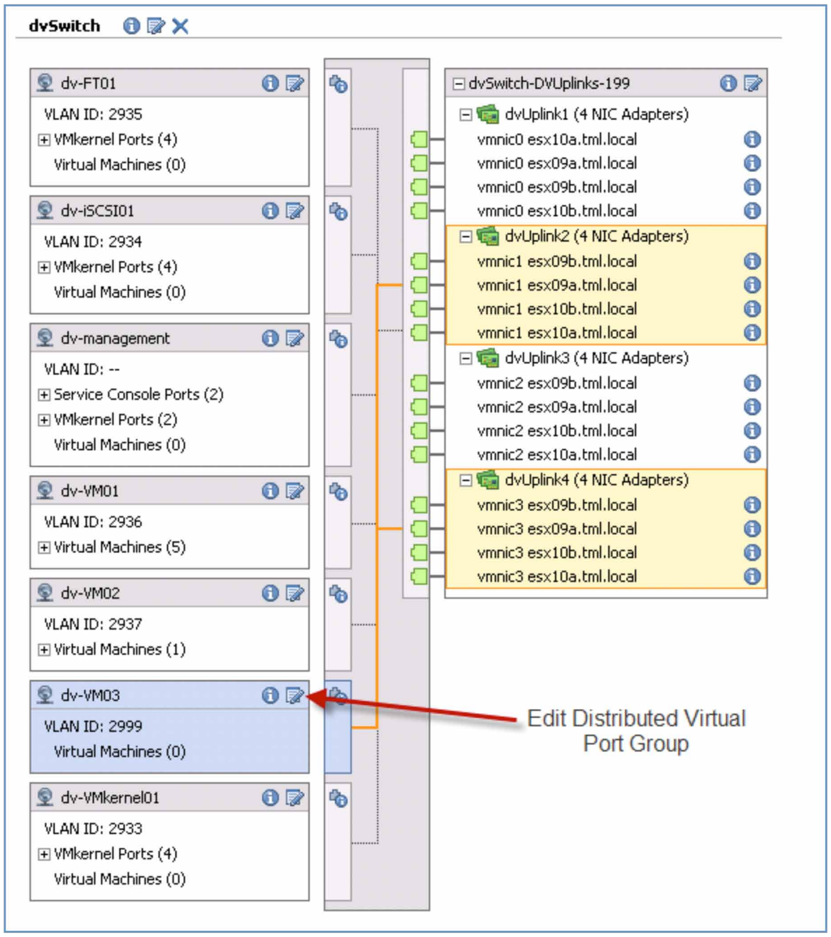
This example where the VLAN changes from 2999 to 2995, you would change this on the Distributed Virtual Port Group in much the same manner you would change this on a Standard Switch Port Group.

Figure 35 shows the vDS and the where we would click to edit the Distributed Port Group settings. Figure 36 shows where you would change the VLAN id in the dv-VM03 Distributed Virtual Port Group settings. Once you change the VLAN ID and click **OK**, the change would be applied to all the hosts almost instantaneously with a minimum of disruption.

Note that any of the Distributed Virtual Port Group parameters could have changed using the same procedure with a single change. Examples of this include:

- Port Security settings
- Ingress and Egress traffic shaping
- Teaming and Failover
- Port Blocking
- VLAN id

Figure 35 - Editing a Distributed Virtual Port Group



dvSwitch

dv-FT01
VLAN ID: 2935
⊞ VMkernel Ports (4)
Virtual Machines (0)

dv-iSCSI01
VLAN ID: 2934
⊞ VMkernel Ports (4)
Virtual Machines (0)

dv-management
VLAN ID: --
⊞ Service Console Ports (2)
⊞ VMkernel Ports (2)
Virtual Machines (0)

dv-VM01
VLAN ID: 2936
⊞ Virtual Machines (5)

dv-VM02
VLAN ID: 2937
⊞ Virtual Machines (1)

dv-VM03
VLAN ID: 2999
Virtual Machines (0)

dv-VMkernel01
VLAN ID: 2933
⊞ VMkernel Ports (4)
Virtual Machines (0)

⊟ dvSwitch-DVUplinks-199

⊟ dvUplink1 (4 NIC Adapters)
vmnic0 esx10a.tml.local
vmnic0 esx09a.tml.local
vmnic0 esx09b.tml.local
vmnic0 esx10b.tml.local

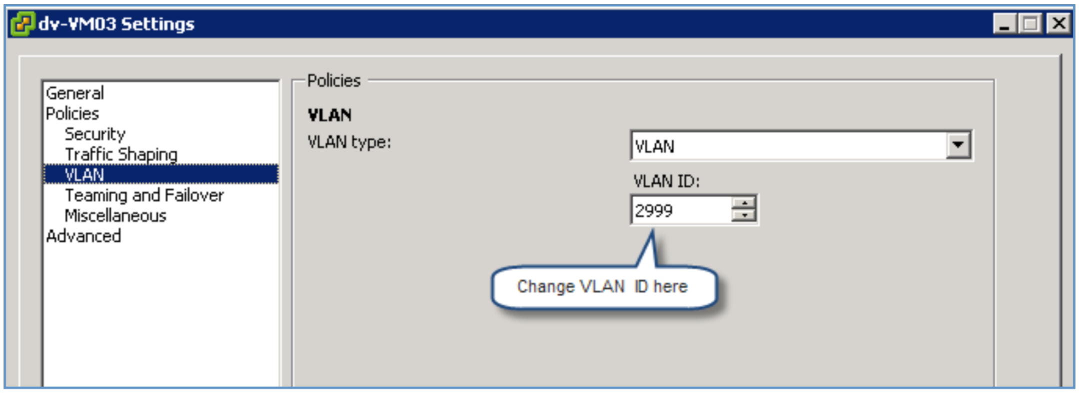
⊟ dvUplink2 (4 NIC Adapters)
vmnic1 esx09b.tml.local
vmnic1 esx09a.tml.local
vmnic1 esx10b.tml.local
vmnic1 esx10a.tml.local

⊟ dvUplink3 (4 NIC Adapters)
vmnic2 esx09b.tml.local
vmnic2 esx09a.tml.local
vmnic2 esx10b.tml.local
vmnic2 esx10a.tml.local

⊟ dvUplink4 (4 NIC Adapters)
vmnic3 esx09b.tml.local
vmnic3 esx09a.tml.local
vmnic3 esx10b.tml.local
vmnic3 esx10a.tml.local

Edit Distributed Virtual Port Group

Figure 36 - Changing the VLAN id on a Distributed Virtual Port Group



VLAN

VLAN type: VLAN

VLAN ID: 2999

Change VLAN ID here

Monitoring, Troubleshooting, and Recovery

The following section covers some basic procedures to monitor the network path through a vDS: understanding the virtual to physical network connections, recovering ESX/ESXi host connectivity, and deleting a vDS.

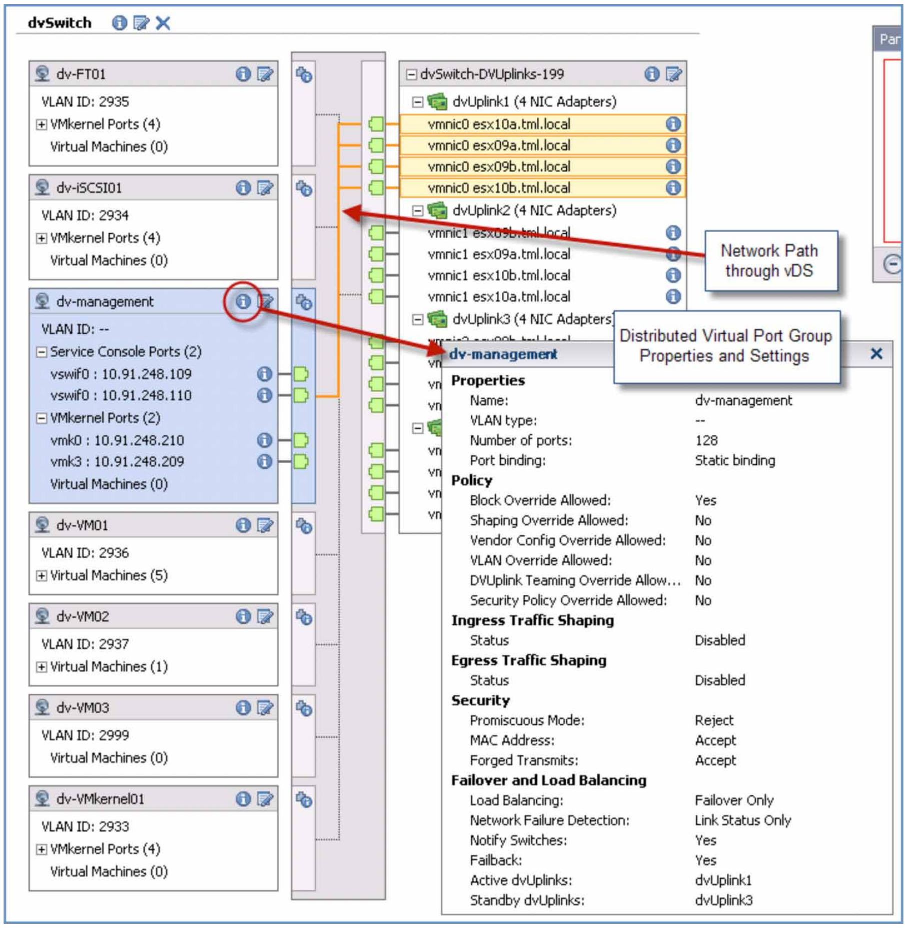
Basic Network Troubleshooting with the vNetwork Distributed Switch

The vNetwork Distributed Switch provides the same troubleshooting feature set as the Standard Switch. In addition, network and server admins will find the vDS configuration panel (**Home > Inventory > Networking**) provides some useful information in troubleshooting the virtual network.

Looking at the vDS for the example environment, (Figure 37), there are a few things to note:

- Clicking on the actual DV Port Group (e.g. dv-management) will highlight the network path defined by the NIC Teaming policy on that DV Port Group. IT can be determined which dvUplinks and which vmnics are used for traffic to and from this DV Port Group (Use the desxtop command described below to see the actual vmnic used by each port as a result of the NIC teaming hash).
- Clicking on the **information icon (i)** shows the properties and settings for that port group. In this example, it can be seen that no VLAN is assigned (so native VLAN in use) for the management ports and that a dvUplink1 was used to map the vmnic0 on all the hosts.

Figure 37 - vDS Panel Showing DV Port Group Information and Network Path



dvSwitch

dv-FT01
VLAN ID: 2935
⊞ VMkernel Ports (4)
Virtual Machines (0)

dv-iSCSI01
VLAN ID: 2934
⊞ VMkernel Ports (4)
Virtual Machines (0)

dv-management
VLAN ID: --
⊟ Service Console Ports (2)
vswif0 : 10.91.248.109
vswif0 : 10.91.248.110
⊟ VMkernel Ports (2)
vmk0 : 10.91.248.210
vmk3 : 10.91.248.209
Virtual Machines (0)

dv-VM01
VLAN ID: 2936
⊞ Virtual Machines (5)

dv-VM02
VLAN ID: 2937
⊞ Virtual Machines (1)

dv-VM03
VLAN ID: 2999
Virtual Machines (0)

dv-VMkernel01
VLAN ID: 2933
⊞ VMkernel Ports (4)
Virtual Machines (0)

⊟ dvSwitch-DVUplinks-199
⊟ dvUplink1 (4 NIC Adapters)
vmnic0 esx10a.tml.local
vmnic0 esx09a.tml.local
vmnic0 esx09b.tml.local
vmnic0 esx10b.tml.local
⊟ dvUplink2 (4 NIC Adapters)
vmnic1 esx09b.tml.local
vmnic1 esx09a.tml.local
vmnic1 esx10b.tml.local
vmnic1 esx10a.tml.local
⊟ dvUplink3 (4 NIC Adapters)

Network Path through vDS

Distributed Virtual Port Group Properties and Settings

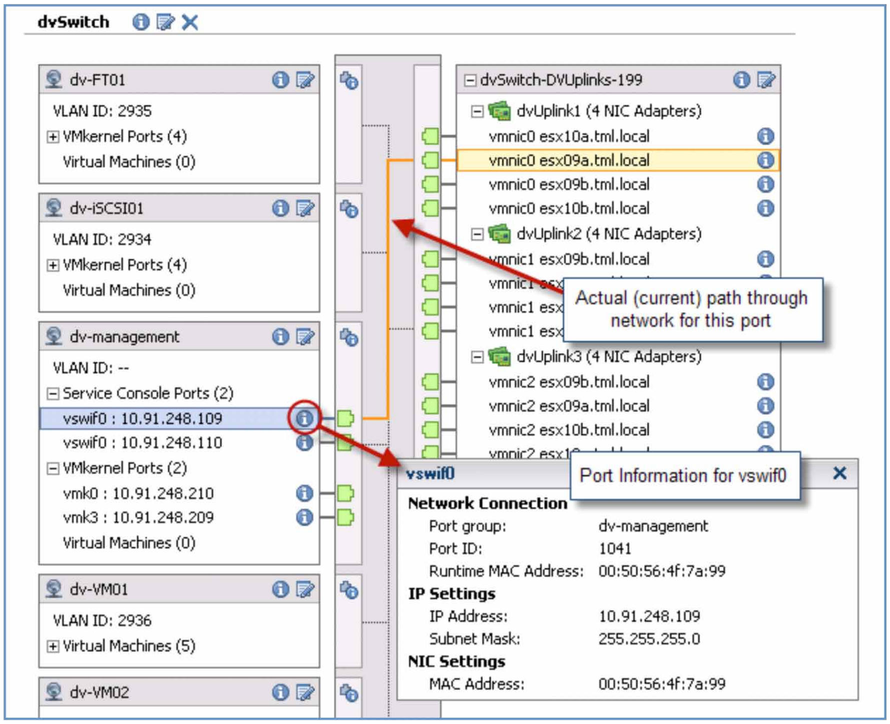
dv-management

Properties	
Name:	dv-management
VLAN type:	--
Number of ports:	128
Port binding:	Static binding
Policy	
Block Override Allowed:	Yes
Shaping Override Allowed:	No
Vendor Config Override Allowed:	No
VLAN Override Allowed:	No
DVUplink Teaming Override Allow…	No
Security Policy Override Allowed:	No
Ingress Traffic Shaping	
Status	Disabled
Egress Traffic Shaping	
Status	Disabled
Security	
Promiscuous Mode:	Reject
MAC Address:	Accept
Forged Transmits:	Accept
Failover and Load Balancing	
Load Balancing:	Failover Only
Network Failure Detection:	Link Status Only
Notify Switches:	Yes
Failback:	Yes
Active dvUplinks:	dvUplink1
Standby dvUplinks:	dvUplink3

You can drill down further by selecting the actual port (Figure 38).

- Clicking on the **port** (in this example, vswif0 on 10.91.248.109) shows the network path through the vDS to the vmnic (vmnic0 on esx09a.tml.local in this example) as defined by the NIC Teaming policy.
- Clicking on the **information icon (i) next** to the port shows the Port ID, MAC address, IP address, and mask.

Figure 38 - vDS Panel showing port information and NIC teaming path through network



Actual (current) path through network for this port

Port Information for vswif0

Network Connection

Port group:	dv-management
Port ID:	1041
Runtime MAC Address:	00:50:56:4f:7a:99

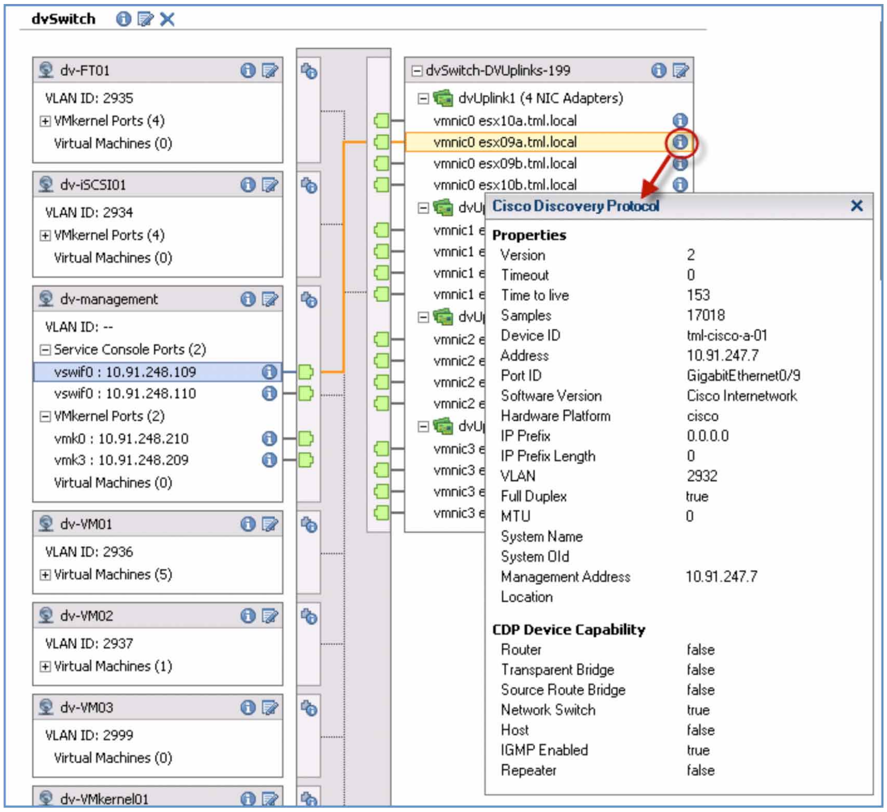
IP Settings

IP Address:	10.91.248.109
Subnet Mask:	255.255.255.0

NIC Settings

MAC Address:	00:50:56:4f:7a:99

Figure 39 - Physical NIC (vmnic) and CDP information



Cisco Discovery Protocol

Properties

Version	2
Timeout	0
Time to live	153
Samples	17018
Device ID	tml-cisco-a-01
Address	10.91.247.7
Port ID	GigabitEthernet0/9
Software Version	Cisco Internetwork
Hardware Platform	cisco
IP Prefix	0.0.0.0
IP Prefix Length	0
VLAN	2932
Full Duplex	true
MTU	0
System Name	
System OId	
Management Address	10.91.247.7
Location	

CDP Device Capability

Router	false
Transparent Bridge	false
Source Route Bridge	false
Network Switch	true
Host	false
IGMP Enabled	true
Repeater	false

You can also look at the physical network connection (Figure 39).

- Clicking on the **information icon (i)** next to the vmnic will show the CDP (Cisco Discovery Protocol) information picked up by that vmnic. In this example, it is shown that vmnic0 on esx09a.tml.local is connected to interface GigabitEthernet 0/9 on the adjacent physical Cisco switch. It is also shown that the management address of the switch and whatfeatures/capabilities are enabled (e.g. multicast, etc).

Note that you need a Cisco switch with CDP enabled for this information to show up on the ESX Server and vCenter Server.

Configuring CDP

Each of the individual ESX hosts can be configured to **down, listen, advertise,** or **both**. CDP can be enabled in two ways:

1. Through the ESX Service Console command line interface. This controls CDP on a host basis.

   The mode is displayed by entering:

   `esxcfg-vswitch –b <vswitch>`

   The CDP mode is configured or changed by:

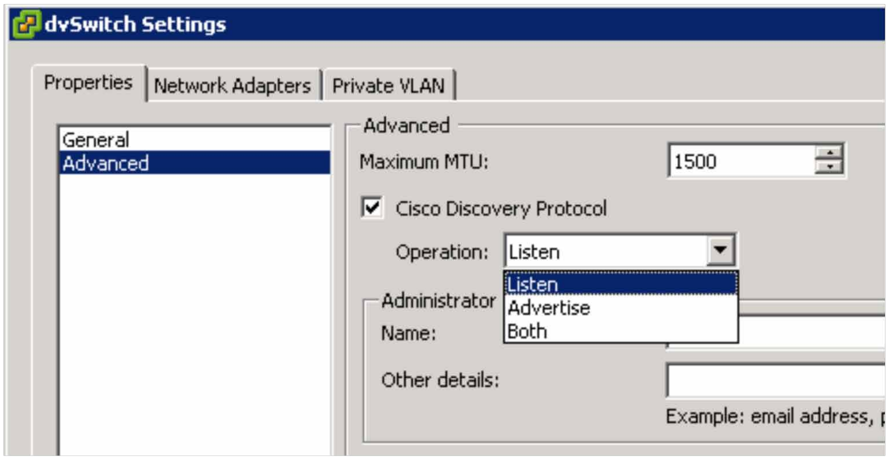
   `esxcfg-vswitch –B <mode> <vswitch> where <Mode>` is one of down, listen, advertise, or both.

2. Through the User Interface. This controls CDP for all hosts encompassed by a vDS.

   From **Home > Inventory > Networking** view, right-click on the vDS and select **Edit Settings**.

   On the popup panel, select **Advanced**; select the **Cisco Discovery Protocol** checkbox and select the desired **Operation**. Listen means ESX will only listen for CDP advertisements from the network; Advertise means ESX will only send CDP advertisements to the physical network; Both means ESX will listen and advertise.

Figure 40 - Configuring CDP on a vDS through the User Interface



Maximum MTU: 1500

☑ Cisco Discovery Protocol

Operation: Listen

For more information on configuring CDP, refer to the ESX Configuration Guide.

Monitoring Hash vmnic Selection in NIC Teams

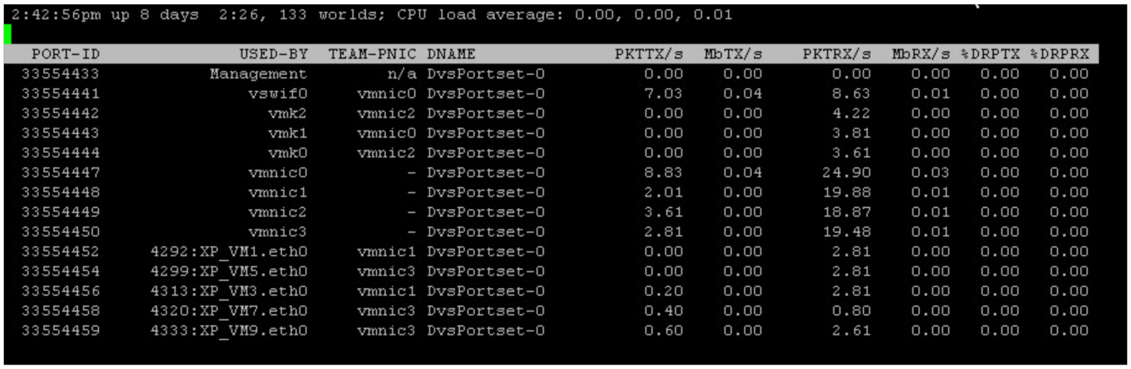
The **esxtop** command from the ESX console can reveal the physical NIC (vmnic) used by virtual port or VM within a NIC team. Figure 41 shows a display capture from an ESX 4 host. This display shows the following:

- PORT-ID represents an internal port number on the virtual switch
- USED-BY column shows what that port number is used by (e.g. VMkernel, VM, etc).
- TEAM-PNIC column shows what physical nic (vmnic) is being used for traffic from that virtual port (the result of the hash within the NIC team).

- The remaining columns indicate the Receive and Transmit traffic rates on those ports.

To use esxtop, type **esxtop** from the ESX console and then type **n**.

Figure 41 - esxtop display showing physical NIC usage by port



```
2:42:56pm up 8 days  2:26, 133 worlds; CPU load average: 0.00, 0.00, 0.01

  PORT-ID              USED-BY  TEAM-PNIC DNAME              PKTTX/s  MbTX/s    PKTRX/s  MbRX/s %DRPTX %DRPRX
 33554433           Management        n/a DvsPortset-0          0.00    0.00       0.00    0.00   0.00   0.00
 33554441               vswif0     vmnic0 DvsPortset-0          7.03    0.04       8.63    0.01   0.00   0.00
 33554442                 vmk2     vmnic2 DvsPortset-0          0.00    0.00       4.22    0.00   0.00   0.00
 33554443                 vmk1     vmnic0 DvsPortset-0          0.00    0.00       3.81    0.00   0.00   0.00
 33554444                 vmk0     vmnic2 DvsPortset-0          0.00    0.00       3.61    0.00   0.00   0.00
 33554447               vmnic0          - DvsPortset-0          8.83    0.04      24.90    0.03   0.00   0.00
 33554448               vmnic1          - DvsPortset-0          2.01    0.00      19.88    0.01   0.00   0.00
 33554449               vmnic2          - DvsPortset-0          3.61    0.00      18.87    0.01   0.00   0.00
 33554450               vmnic3          - DvsPortset-0          2.81    0.00      19.48    0.01   0.00   0.00
 33554452      4292:XP_VM1.eth0     vmnic1 DvsPortset-0          0.00    0.00       2.81    0.00   0.00   0.00
 33554454      4299:XP_VM5.eth0     vmnic3 DvsPortset-0          0.00    0.00       2.81    0.00   0.00   0.00
 33554456      4313:XP_VM3.eth0     vmnic1 DvsPortset-0          0.20    0.00       2.81    0.00   0.00   0.00
 33554458      4320:XP_VM7.eth0     vmnic3 DvsPortset-0          0.40    0.00       0.80    0.00   0.00   0.00
 33554459      4333:XP_VM9.eth0     vmnic3 DvsPortset-0          0.60    0.00       2.61    0.00   0.00   0.00
```

ESX/ESXi Host Network Recovery

This section describes how to recover network connectivity to an ESX or ESXi host after configuration failure or mistake.

ESX Host Virtual Network Recovery

The recovery procedure for an ESX host involves moving the management vswif interface to a new temporary vSS. Management access to the server is required through an ILO interface or KVM physically attached to the server. After management connectivity is restored, use the vSphere Client to continue virtual network configuration.

Step 1: Logon to ESX host.

Step 2: Create a new temporary vSS (tmpSwitch) and Port Group (vswifPg)

```
esxcfg-vswitch -a tmpSwitch
esxcfg-vswitch -A vswifPg tmpSwitch
```

Step 3: Move uplink from vDS to vSS

```
esxcfg-vswitch -l    (to get DVSwitch, DVPort, and vmnic names)
esxcfg-vswitch -Q vmnic0 -V <dvPort> <dvSwitch>   (unlink vmnic0 from vDS)
esxcfg-vswitch -L vmnic0 tmpSwitch   (link to vswitch)
```

Step 4: Move vswif from vDS to vSS

```
esxcfg-vswif -l (get vswif IP address, netmask, dvPort id, etc.)
esxcfg-vswif -d vswif0
esxcfg-vswif -a vswif0 -i <ip address> -n <netmask> -p vswifPg
```

Check or edit the default gateway address by editing /etc/sysconfig/network or adding default gateway address with:

```
route add default gw <gateway address>
```

A list of commands for the ESX command line interface is published in Chapter 6 of the ESX 4.0 Configuration Guide (available at http://www.vmware.com/support/pubs/). To control console output to one page at a time by adding the | **more** suffix to the commands. For example:

```
esxcfg-vswitch –l | more
```

ESXi Host Virtual Network Recovery

ESXi hosts feature a menu driven user interface on the VMkernel management port. There is a menu item for restoring the management network. This moves the management network and uplinks to a vSS. Ensure the management default gateway is specified correctly (on the same network as the management interface).

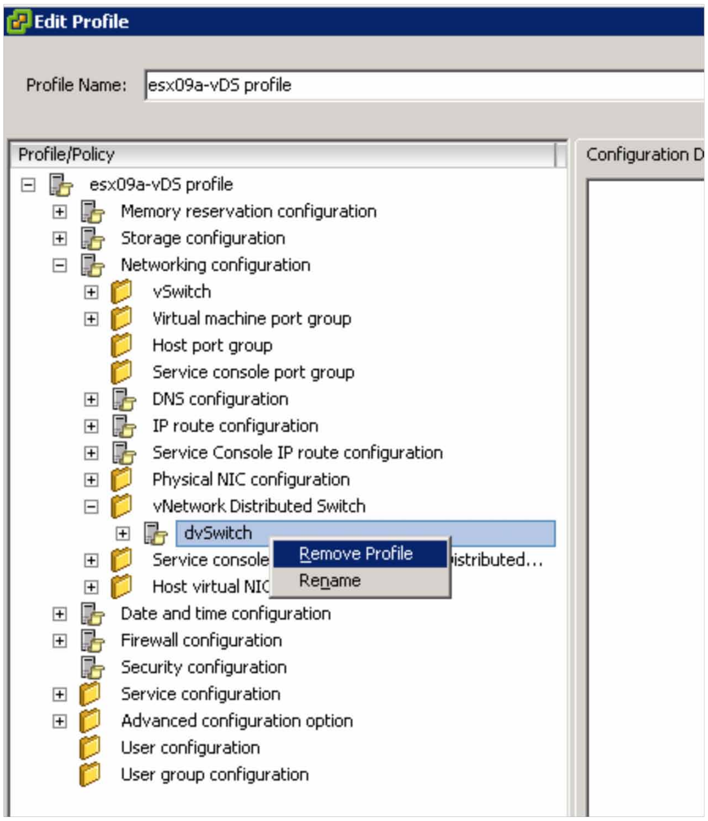
Removing a Host from a vDS

A vDS can be removed from an ESX or ESXi host using Host Profiles. The procedure is as follows:

1. Move the virtual ports and VMs to another vSS or vDS with network connectivity
2. Create a Host Profile of the host
3. Edit the Host Profile and expand **Network Configuration** and then **vNetwork Distributed Switch**
4. Right click on the vDS to be deleted and select **Remove Profile** and then save with **OK**. See Figure 42.
5. Put host in Maintenance Mode
6. Apply host profile

Any vmnics attached to the vDS on that host are then freed for assignment to another vSS or VDS.

Figure 42 - Editing a Host Profile to remove a vDS



Edit Profile

Profile Name: esx09a-vDS profile

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com