IBM System Networking

Software Defined Network for Virtual Envirmonments

Version 1.0, VMware Edition

User Guide

First Edition (June 2013)

Contents

Preface

This *User Guide* describes how to configure and use the IBM System Networking Software Defined Network for Virtual Envirmonments (SDN VE) version 1.0 to provide virtualization of the physical network within a VMware-enhanced datacenter using IBM Distributed Overlay Virtual Ethernet (DOVE) technology.

Who Should Use This Guide

This guide is intended for network installers and administrators engaged in configuring and maintaining a complex network. The administrator should be familiar with general Ethernet concepts and Layer 2 switching. They should also be familiar with the required VMware vCenter, vSphere, and ESX products and virtualization concepts.

What You'll Find in This Guide

This guide will help you plan, implement, and administer IBM SDN VE software. Where possible, each section provides feature overviews, usage examples, and configuration instructions. The following material is included:

Part 1: Getting Started

This material is intended to help those new to this product understand the basics of SDN VE installation and management. This part includes the following chapters:

- Chapter 1, "IBM SDN VE Introduction," provides a conceptual overview of the SDN VE solution, and describes the prerequisites and general tasks for SDN VE installation.
- Chapter 2, "Installing DMC Modules," covers specific instructions for the installation and initial configuration of the DOVE Management Console (DMC) software which provides the core intelligence of the SDN VE solution.
- Chapter 3, "Installing DSA Modules," provides specific instructions for the installation and initial configuration of the DOVE Service Appliance (DSA) software which provides network connectivity to both virtual and physical network elements.
- Chapter 4, "Installing the DS 5000V," provides specific instructions for the installation and initial configuration of the Distributed Switch 5000V software which provides virtual switching within a VMware virtual datacenter.
- Chapter 5, "Virtual Network Configuration," provides specific instructions and examples for configuring elements of the virtual network.

Part 2: Command Reference

This section lists each command, together with the complete syntax and a functional description, from the Command-Line Interface (CLI).

- Chapter 6, "Command Basics," provides an overview of the command syntax, including command modes, global commands, and shortcuts.
- Chapter 7, "DMC Show Commands," provides an alphabetic list of DOVE Management Console (DMC) commands for collecting system configuration and statistics information.
- Chapter 8, "DMC Configuration Commands," provides an alphabetic list of DMC configuration commands.

- Chapter 9, “DSA Show Commands,” provides an alphabetic list of DOVE Service Appliance (DSA) commands for collecting system configuration and statistics information.
- Chapter 10, “DSA Configuration Commands,” provides an alphabetic list of DSA configuration commands.

Part 3: Appendices

- Appendix A, “Known Issues.”
- Appendix B, “Getting Help & Technical Assistance,” describes how to obtain product support.
- Appendix C, “Notices.”

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1. Typographic Conventions

Typeface or Symbol	Meaning	Example
ABC123	This italicized body type shows book titles, special terms, or words to be emphasized.	Read your *User's Guide* thoroughly.
ABC123	This plain, fixed-width type is used for names of commands, files, and directories used within the body of the text.	View the `readme.txt` file.
	It also depicts on-screen computer output and prompts.	`host#`
ABC123	This bold, fixed-width type appears in command examples. It depicts text that must be typed in exactly as shown.	`host#` **`show config`**
< >	Angled brackets appear in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.	If the command syntax is: **`ping`** *<IPv4 address>* You might enter: **`ping 192.32.10.12`**
[ ]	Square brackets depict optional elements within commands. These can be used or excluded as the situation demands. Do not type the brackets.	`host#` **`ls`** [**`-a`**]
{**A**|**B**}	Curled braces and vertical bars are used in command examples where there are multiple choices. Select only one of the listed options. Do not type the braces or bars.	If the command syntax is: **`set`** {**`left`**|**`right`**} You might enter: **`set left`** Or: **`set right`**
AaBbCc123	This bold type depicts menus, buttons, and other controls that appear in Web browsers and other graphical interfaces.	Click the **Save** button.
A > B	This bold type with an angled right-bracket indicates nested menu items in a graphical interface.	Select **File > Save**.

How to Get Help

If you need help, service, or technical assistance, visit our web site at the following address:

http://www.ibm.com/support

The warranty card received with your product provides details for contacting a customer support representative. If you are unable to locate this information, please contact your reseller. Before you call, prepare the following information:

- Serial number of the switch unit
- Software release version number
- Brief description of the problem and the steps you have already taken
- Technical support dump information (`show tech-support`)

Part 1: Getting Started

Chapter 1. IBM SDN VE Introduction

Solution Overview

The IBM System Networking Software Defined Network for Virtual Envirmonments (SDN VE) version 1.0, VMware Edition, is part of the IBM's solution for Software Defined Networking (SDN). SDN represents a major advance in enterprise communications that creates a new network paradigm that separates network control logic from the underlying network hardware.

With SDN, instead of having to directly configure each connected device that makes up a network, administrators can dynamically establish multiple networks. They can also allocate bandwidth and route data flows for optimized performance using high-level control programs. By overlaying virtual networks onto physical networks, administrators can make existing infrastructure more adaptable to different workloads. The result is an agile, optimized, scalable network that is responsive to the needs of the business.

The SDN VE network overlay solution supplies a complete implementation framework for network virtualization. It supplies a core component of SDN architecture, which is fully deployable for data center expansion.

SDN VE takes a host-based overlay approach, which achieves advanced network abstraction that enables application-level network services in large-scale multi-tenant environments. It provides a multi-hypervisor, server-centric solution comprising multiple components that overlay virtual networks onto any physical network that provides IPv4 connectivity. The software is designed to support multi-vendor data center environments.

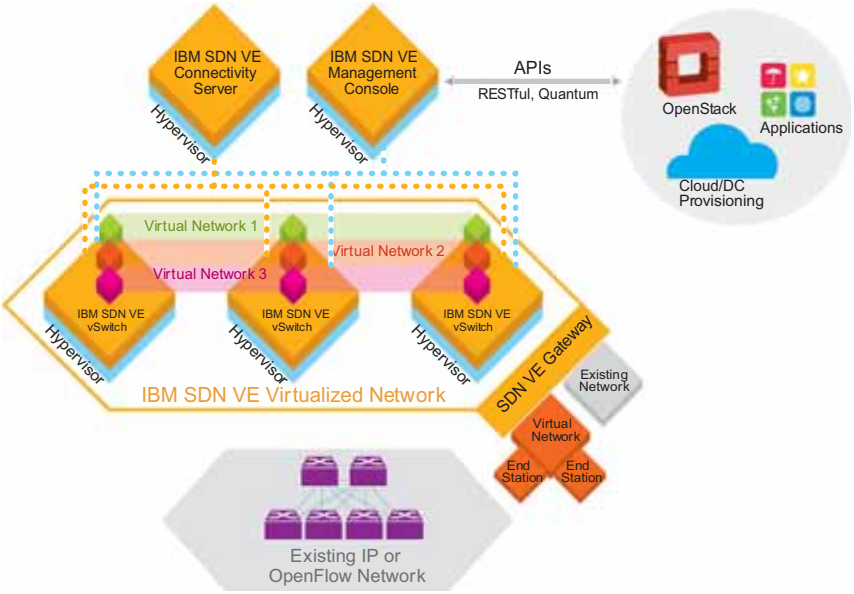


Figure 1. IBM SDN VE is a multi-hypervisor virtual network overlay that uses existing IPv4 infrastructure

Although implementing the software does not require changes to physical infrastructure, the hypervisor must be updated. Specifically, implementing the SDN VE VMware Edition requires an SDN VE Virtual Switch (an upgrade to the IBM Distributed Virtual Switch 5000V) to be resident in VMware. SDN VE VMware Edition is packaged for easy installation using VMware install and update tools.

SDN VE Element

The SDN VE solution is made up of four software components that work in combination to provide effective host-based network virtualization.

- An Distributed Switch 5000V (5000V) is software that resides in the hypervisor. It serves as the start and end point of each virtual network. The 5000V provides Layer 2 and Layer 3 network virtualization over a UDP overlay, and implements the data path of the virtual network. The virtual switch also performs control plane functions to support virtual machine (VM) address auto discovery, VM migration and network policy configuration.
- A connectivity service disseminates VM addresses to the virtual switches participating in an SDN VE virtual network. The connectivity service software is deployed as a cluster of virtual appliances.
- A management console is the centralized point of control for configuring SDN VE. It configures each virtual network, controls policies and disseminates policies to the virtual switches. It also helps administrators manage individual virtual networks. The software resides on a server as a virtual appliance.
- VLAN- and IPv4-based gateways enable SDN VE to establish interoperability with networks and servers that are external to the SDN VE environment. For Layer 2 networks, SDN VE provides VLAN-based gateways. For Layer 3 networks, the software provides IPv4-based gateways.

Benefits of the IBM SDN VE Solution

The SDN VE solution offers data center managers many ways to expand services and control costs. Benefits of the software include:

- Virtualizes existing IPv4 networks with no change to the underlying physical network infrastructure
- Automates network provisioning and simplifies administration, which can help reduce operating expenses
- Expedites data center consolidation by allowing existing network addresses to be retained
- Enables large-scale multi-tenancy with independent management and optimization of multiple virtual networks
- Improves server resource utilization and return on investment by removing the network as a bottleneck to increased VM density
- Provides API-based programmatic access to virtual networks, which allows data center provisioning platforms and network services to use virtual networks as a service or as an infrastructure

No Disruption to Existing IPv4 Networks

No CIO wants to replace a data center network. In most large-scale data centers, network administrators strive to wire the network one time then operate and maintain it without change. The fact is, changing the underlying physical infrastructure to support new business application requirements is hard to do and typically takes days to weeks to complete. This is a central problem data center managers must resolve. When compute and storage resources can be provisioned rapidly but network connectivity cannot, it can negatively impact business agility.

SDN VE can help data center managers increase business agility by enabling rapid provisioning of virtual network services without disrupting existing physical assets. The software does not require any changes to existing networks to operate, a valuable attribute that simplifies adoption.

The only requirement to implement SDN VE is a simple one. The physical network infrastructure on which the software is overlaid must be capable of providing IPv4 address-based connectivity. Every typical enterprise data center network supports this capability.

SDN VE efficiently overlays virtual networks onto existing networks, thus decoupling application connectivity from the physical network infrastructure. This enables a “wire once” physical network that can support multiple SDN VE virtual networks which can be flexibly managed and controlled through highly available clusters of IBM SDN Connectivity servers and the IBM SDN Management Console. This architecture separates the control plane from the data plane, a central tenet of SDN.

SDN VE operates by adding a distinct header to packets sent by VMs. Each SDN VE data transfer is just an ordinary IPv4 packet sent to the existing switches in the data center network and the switches can use existing IPv4 forwarding routes and tables. Devices continue to operate at line rates. The SDN VE solution builds on the network that is already in place, and provides the flexibility to create and manage virtual networks on demand.

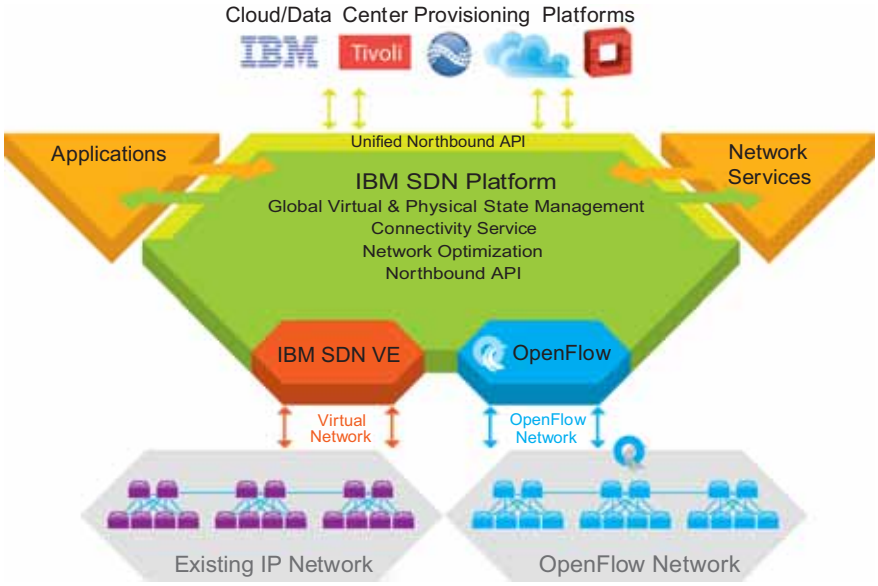


Figure 2. IBM SDN VE abstracts the underlying network and presents it to applications as either a service or as an infrastructure

Extending the VM Strategies into the Network

SDN VE is a logical extension of the virtualization trend that has become the dominant feature in the data center. The software extends the efficiency and productivity advantages achieved with server virtualization to the process of network provisioning and management. These advantages allow data centers to be more:

- Efficient, because SDN VE improves resource use. It allows secure, dedicated virtual networks to be created quickly and easily, without requiring changes to the underlying physical infrastructure.

- Agile, because SDN VE cuts network provisioning time from days to minutes. With SDN VE, you can establish secure virtual networks as easily as starting up VMs.
- Scalable, because SDN VE offers data center managers the scalability needed for current and future growth. Up to 16 million networks can be specified in the architecture. The first release supports 16,000 virtual networks.

High Availability

Enterprise data centers maintain uncompromising standards for high availability, which reflects the value that data center operations contribute to the enterprise. In many cases, the data center is one of the most valuable components in the business because the enterprise cannot function if the data center is down. SDN VE supports enterprise needs for high availability with customizable, redundant component design.

Two or more active SDN VE Connectivity Servers control each virtual network. The number of SDN VE Connectivity Servers that can be assigned to individual virtual networks is user-configurable. This ensures that the user can select the level of high availability needed for a given virtual network. This redundant design allows the state of each SDN VE Connectivity Server to be replicated in at least one other instance of the SDN VE Connectivity Server at all times. The SDN VE Management Console provides high availability in Active and Standby modes. One instance operates in Active mode, and the other functions in Standby mode. If an Active SDN VE Management Console experiences a failure or outage, automatic failover to the Standby SDN VE Management Console occurs. SDN VE Gateways also support redundancy, allowing failover in the event of an outage. In these ways, SDN VE is a high-performance, high availability solution.

Enhanced Multi-tenancy for Cloud Providers

The gains in adopting SDN VE are far greater than employing VLANs. With SDN VE you can create secure, scalable multi-tenant networks with individual network control. Each virtual network created with SDN VE can be managed individually using the application programming interface (API) the software provides. In addition, you get greater scalability with SDN VE: A traditional network is physically limited to 4,096 VLANs, and requires configuration of end-to-end VLANs on some or all physical devices in the network. With SDN VE, the maximum number of VLANs that can be supported increases from a physical limit of 4,096 networks to an architectural limit of 16,000,000. The first release of SDN VE VMware Edition supports 16,000 virtual networks.

Cloud providers that need to support multiple customers with dedicated, reliable, secure and scalable networks, can deploy SDN VE to help supply these services with increased cost effectiveness and efficiency.

Datacenter Consolidation

Datacenter consolidation is a common practice among large enterprises today because of the increased economy and efficiency that can be gained. Consolidation can also be necessitated by mergers and acquisitions if because the acquiring company wants to ensure that all customers receive the same service experience. One difficulty of consolidation is in combining IPv4 addresses. Redesigning complete network schemas is an exceptionally complex and time-consuming challenge. SDN VE resolves this problem by reusing existing IPv4 addresses. In fact, the network address of each VM in an SDN VE virtual network is not exposed to the physical network. SDN VE only exposes one network address per NIC. This greatly simplifies the process of creating and deploying virtual networks on demand.

Maximizing Servers

VMs require real network connections. However, since it is much easier to create VMs than it is to network them, your network resources can be exhausted before you can use your servers to the fullest extent. Maximizing server use is a principal reason to implement SDN VE. With the software in place, VM density can be increased to the limits of memory, and processor cycles and server virtualization can continue without concern for VM network bottlenecks. With SDN VE, you can establish a “wire-once” data center network environment with expansion capacity for future growth and increased virtualization.

Optimizing Provisioning with Programmable APIs

The SDN VE solution provides programmatic access to virtual network functions using RESTful APIs, which can provide web services to any client program able to transmit messages using the HTTP protocol. SDN VE also supports the OpenStack Quantum API, which is a network abstraction that allows OpenStack to use the underlying network as the infrastructure without requiring it to have knowledge of the underlying resources.

The Software-Defined Environment

In the era of Smarter Computing, entire data center infrastructures will become as programmable as individual systems are today. Compute, storage, network and middleware components will be tuned to the workload, endlessly scalable and adaptable to dynamic workload demands. The datacenter, in short, will be efficient, flexible, purpose-built and aligned with the needs of the business. With SDN VE software, secure multi-tenant network virtualization and abstraction of physical assets are not merely capabilities your network will have in the future. They are benefits you can achieve with the network you have today.

Components

The SDN VE solution requires the following components:

- VMware elements
  - VMware vCenter

    This VMware product resides on a server within the datacenter. It provides a centralized tool for installing, managing and synchronizing hypervisors, virtual machines (VMs), and virtual distributed switches (vDS) on host servers throughout the datacenter.

  - VMware vSphere Client or vSphere Web Client

    This VMware vSphere Client resides on administrative client devices. It provides the server administrator or network administrator with rich, remote access to vCenter management tools. The vSphere Web Client provides similar access via your web-browser interface.

  - VMware ESX 5.0 or 5.1

    These VMware hypervisor products reside on individual host servers within the datacenter. They provides the software infrastructure for installing, running, and managing VM and vDS elements on the hosts.

- SDN VE elements
  - DOVE Management Console (DMC)

    This IBM System Networking software resides on two VMware VMs on different hosts within the virtual datacenter. Together, they provide the resilient core intelligence for the Distributed Overlay Virtual Ethernet (DOVE), unifying the operation of various VM-based service appliance modules that form the fabric of the distributed virtual network.

  - DOVE Service Appliance (DSA)

    This IBM System Networking software resides in multiple VMware VMs. Each has the capacity to become a DCS or a DGW as described below.

  - DOVE Connectivity Service (DCS)

    These IBM System Networking software modules collect and process network information pertaining to nearby VMs, gateways and virtual switches in the virtual datacenter. Domain information is synchronized among partner modules within the distributed virtual network.

  - DOVE Gateways (DGW)

    These IBM System Networking software modules can serve as a gateway to join the virtual network to an external, non-virtual network associated either with a specific port in the physical network or with legacy VLAN broadcast domains.

- IBM DS 5000V elements

  The 5000V is a versatile vDS solution. Though it can be used independently to provide general virtual switching within a VMware virtual datacenter (outside of the SDN VE solution), it is a required element within SDN VE solution:

  - 5000V vDS Host Modules

    This IBM System Networking software resides in participating VMware ESX hypervisors on host servers within the virtual datacenter. It implements a vDS portset as defined in the VMware vDS API and acts a virtual network switch for the given host server. At its core, it forwards frames based on destination MAC addresses, controlling Layer 2 access to and from the associated VMs. It also provides advanced switching features such as VLANs, IGMP snooping, etc. In the SDN VE solution, the 5000V vDS host modules act as Tunnel End-Points (TEPs).

  - 5000V Controller

    This IBM System Networking software resides in a VM within the datacenter. It works in conjunction with SDN VE and VMware modules to unify the 5000V vDS host modules associated with a specific vDS into an aggregate superswitch.

Prerequisites

The following must be provide prior to SDN VE installation:

- VMware vCenter Server must be installed and operational in your network (see the documentation provided with your vCenter product).

- All host servers which take part of the SDN VE solution must be installed and operational, and include the following:
  - There should be more than 1 host for vMotion.
  - Each host must have a minimum of one 1G or 10G physical NIC.
  - Each host must have IPv4 Layer 2/Layer 3 network connectivity to the vCenter and all host servers which will participate in their virtual network domain. IPv6 is not presently supported.
- In addition to the general host requirements:
  - Each host server that includes a DMC, DSA, or 5000V vDS host module must have ESX 5.0 or 5.1 installed and operational.
  - The host server that includes the 5000V Controller, it is highly recommended that VMware High Availability and/or VMware Fault Tolerance features be configured to protect the virtual switch against downtime or data loss.
  - Each host server that includes a 5000V vDS host module must also have a valid VMware Enterprise Plus license installed.
- VMs for DMC, DCS, and DGW modules must include the following:
  - For DMC, two VMs on different ESX hosts are required.
  - For DCS, two VMs on different ESX hosts are required (and three are recommended).
  - For DGW, two VMs on different ESX hosts are required.
  - For the 5000V Controller, one VM is required.
  - For the 5000V vDS host module, one VM is required for each host that will include a vDS portset.
  - Each VM used SDN VE entities must have a minimum allocation of 2 GB of memory.

The following SDN VE software files are required:

- Open Virtual Appliance (OVA) files for—
  - DOVE Management Console
  - DOVE Service Appliance (DSA)
  - DS 5000V Controller
- VIB offline bundle file file for 5000V vDS host module. This file includes the vSphere Installation Bundle (VIB).

Installation Summary

The following tasks summarize the SDN VE installation process and are covered in detail in the installation chapters:

Installing DMC Modules

- Using VMware vSphere to deploy the DMC OVA file to VMs on two hosts.
- Initial DMC setup, including:
  - Starting the modules
  - Logging in to the CLI
  - Setting each module's IPv4 parameters
  - Establishing high-availability for system resilience

Installing DSA Modules

- Using VMware vSphere to deploy the DSA OVA file on at least five VMs.
- Initial DSA setup, including:
  - Starting the modules
  - Logging in to the CLI
  - Setting each module's IPv4 parameters
  - Attaching the modules to the DMC cluster
  - Specifying a connectivity or gateway role for each module

Installing the DS 5000V

- Using VMware vSphere to deploy the DS 5000V Controller OVA file on a VM.
- Initial 5000V setup, including:
  - Starting the module
  - Logging in to the CLI
  - Setting the module's IPv4 parameters
  - Creating a global vDS instance in the vCenter
  - Attaching the module to the DMC cluster

Configuration Summary

The following tasks summarize the SDN VE configuration process and are covered in detail in the network configuration chapter:

Configure the overlay network

- Create domains
  - Create networks
  - Define network address space
  - Define policies
  - Export network configuration to the virtual switch
- Externalize the overlay networks
  - Configure VLAN Gateways
  - Configure External Gateways
  - Configure Gateway Interfaces
- 5000V vDS Host Module
  - Install 5000V vDS Host Modules
  - Configure the Underlay (Physical) Networks
  - Attach ESXi Hosts to the vDS
  - Configure Tunnel End-Points
- Attach End Systems

Chapter 2. Installing DMC Modules

The DOVE Management Console (DMC) provides the core intelligence that unifies the operation of the individual appliance modules that will be installed on the participating host servers. DMC modules must be installed and initialized on two different hosts for high-availability (HA) resilience as covered in this chapter.

Deploying the DMC Software

Though deploying DMC software can be accomplished using either the VMware vSphere Client, vSphere Web Client, or OVF Tool, the procedure shown in this *User Guide* depicts only the vSphere Client. If using one of the other tools, extrapolate from the information provided.

Follow these steps to deploy the required DMC modules:

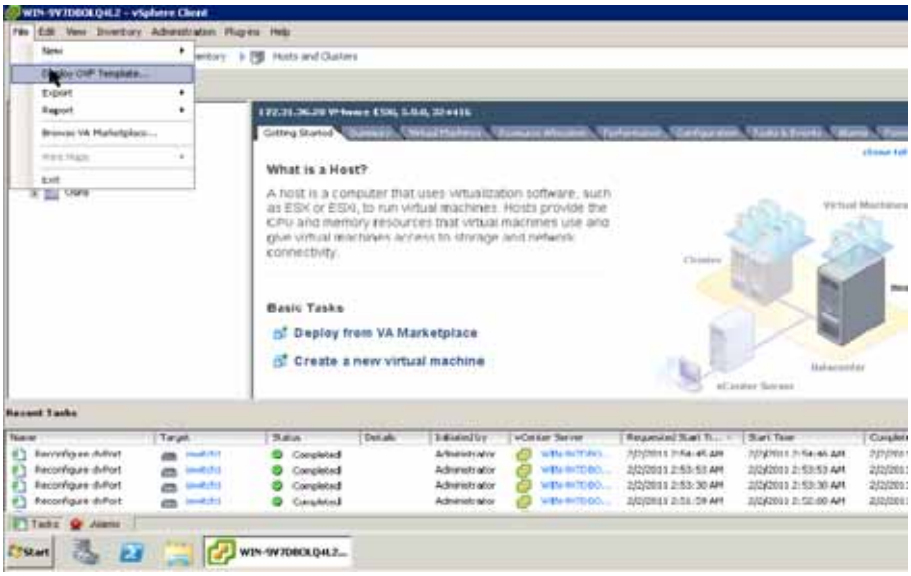
1. Download the DMC OVA file from IBM.
2. Place the OVA file on a system that has access to the VMware vSphere Client (such as an administrative laptop).

Note: Two DMC modules on different hosts are required. Perform the remaining steps once for a *primary* DMC, and again for a *secondary* DMC on another host.

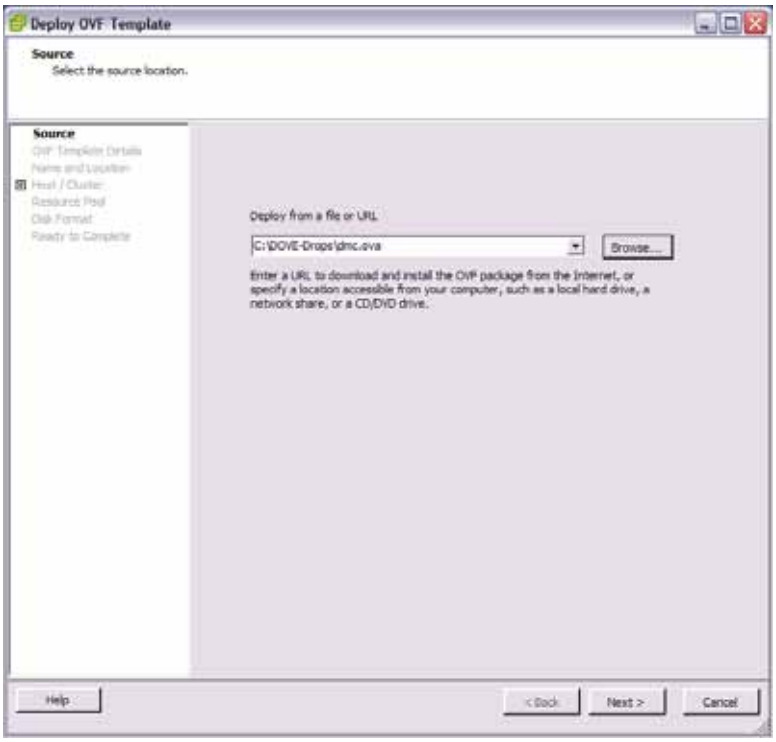
3. Select an ESX host on which to deploy the DMC.

   The DMC host merely provides an environment in which the SDN VE system will run. It is not required to participate as a vDS host and may be a different class of device than those where the vDS host modules will be installed. The primary requirement is for the DMC host to have Layer 3 connectivity to the designated vCenter and participating DSA modules.

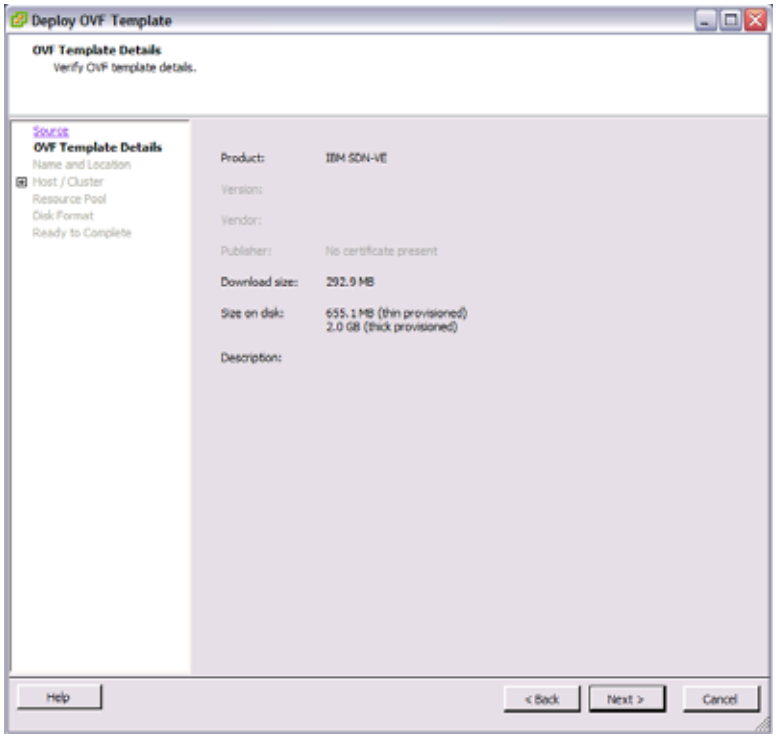
4. Launch the VMware vSphere Client and connect either to the vCenter that manages the host where the DMC will be deployed or directly to the ESX host.
5. From the vSphere Client, select the target ESX host and choose **File > Deploy OVF Template** as shown below:



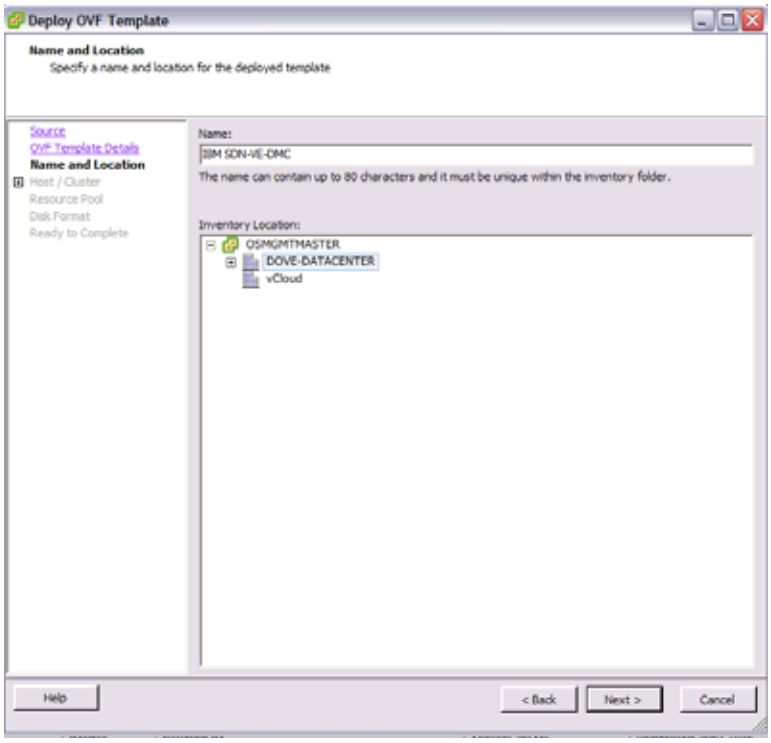
6. Select the location where the OVA file is stored and click **Next**.



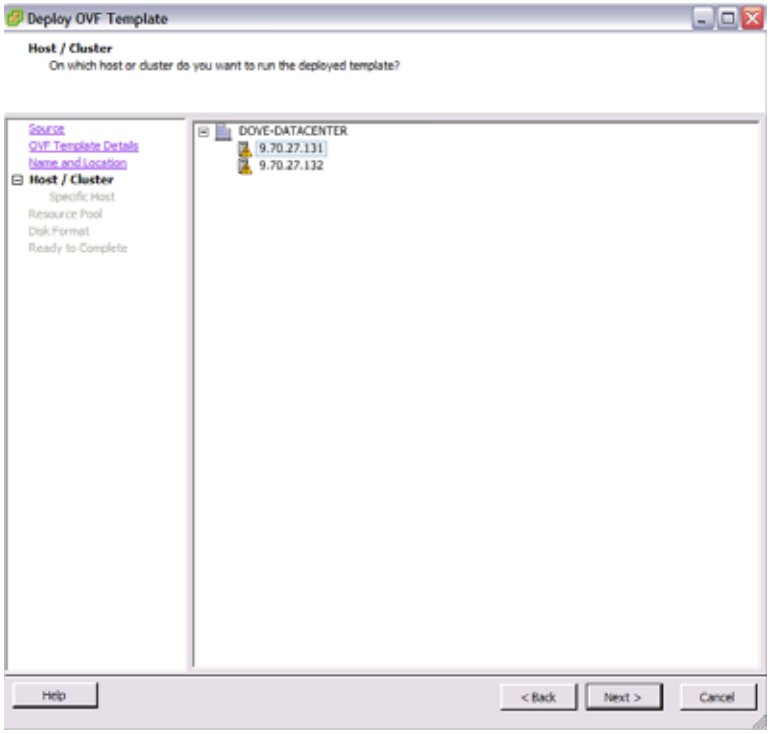
7. Verify the OVA details and click **Next**.



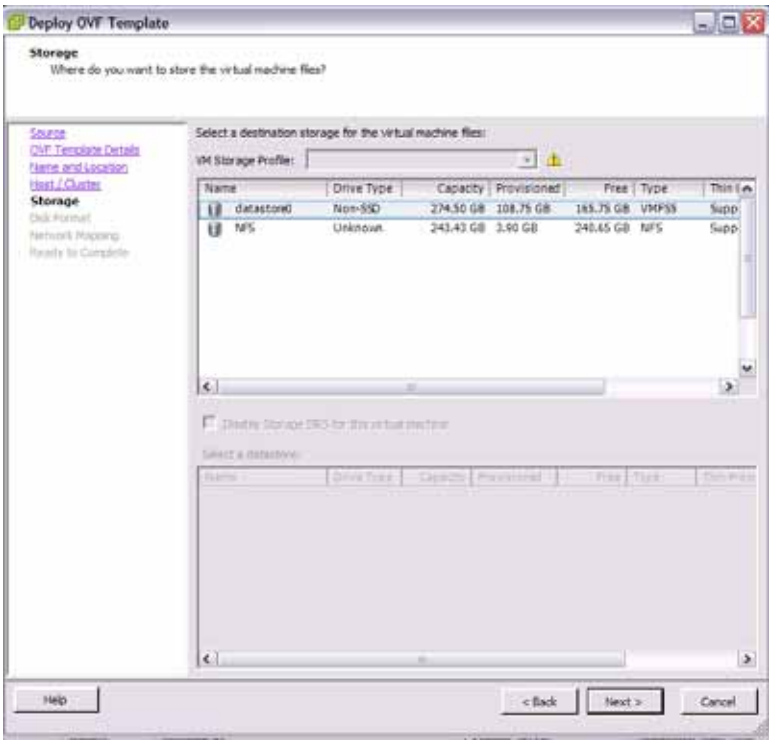
8. Provide a name for the DMC module and click **Next**.



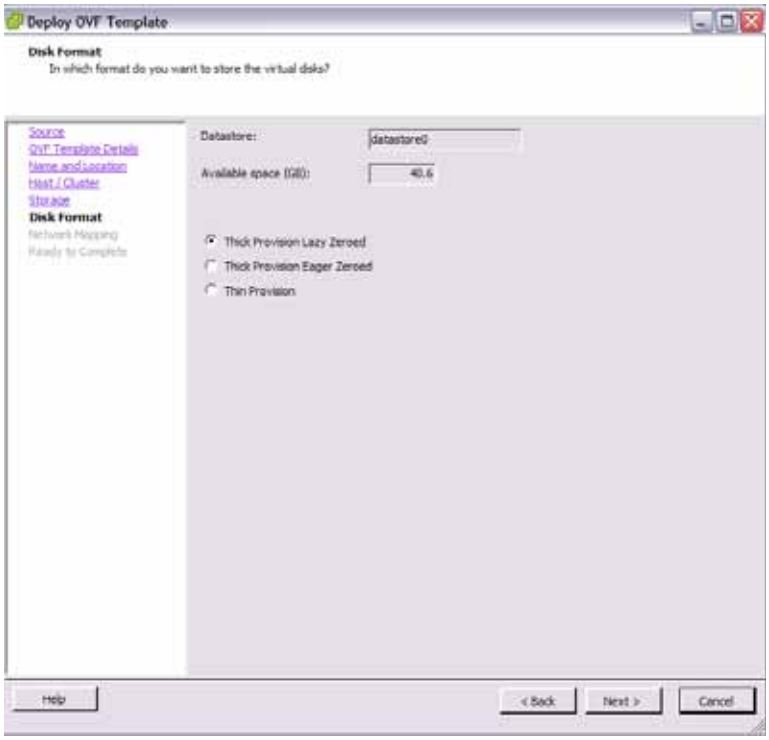
9. Specify the host or cluster on which to deploy the DMC and click **Next**.



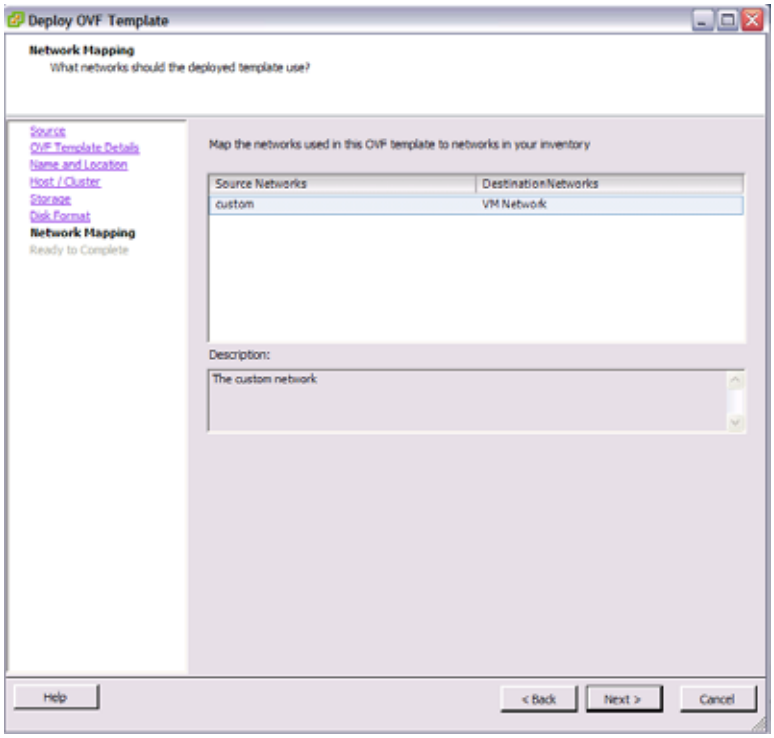
10. Specify a location on the VM where DMC files should be stored, and click **Next**.



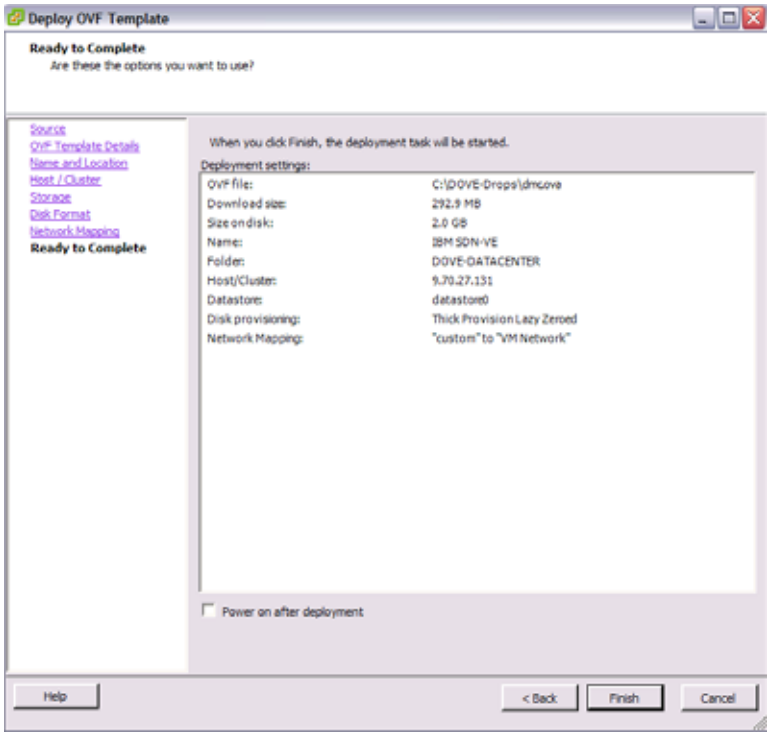
11. Select a disk format and click **Next**. The recommended format is Thick Provisioned Lazy Zeroed.



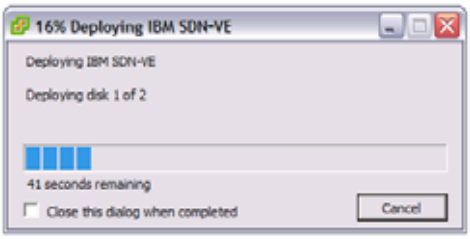
12. Map the network for DMC controller use and click **Next**.



13. Verify the specified options, select the “Power on after deployment” option, and click **Next**.



This will initiate the DMC module VM deployment:



The DMC VM will power on when deployment is complete, and the IBM SDN VE management console will appear.

Initial DMC Setup

After installing primary and secondary DMC module software on VM hosts, each DMC must be manually configured by entering commands into the built-in Command-Line Interface (CLI). Initially, the CLI can be accessed only through each DMC VM console on the vSphere Client. Later, if desired, the CLI can be accessed via remote SSH connection or configuration can be performed via the browser-based interface (BBI).

Note: Configuration of the DMC must be performed solely through the DMC module, and not through the vCenter interface (even in cases where the vCenter interface seems to allow it). However, host operations (such as adding ESX hosts and uplinks or assigning VM network interfaces to vDS ports or profiles) must be done through the vCenter interface.

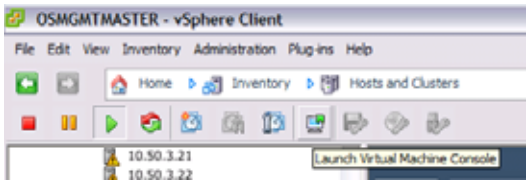
Perform the following initial DMC setup for both the primary and secondary DMC modules.

Start the DMC Module

When following the provided installation instructions, the DMC module automatically starts when the VM is powered on.

However, to manually access the console under other conditions, use the following procedure:

1. Log-in to the VMware vCenter via your vSphere Client.
2. Right-click on the DMC VM and select the option to “Open Console.” Alternately, you can click on the Console icon.



The VM console for the DMC will appear.

Examine the License Agreement

The first time the DMC is started, you will be prompted to read the Software Licence Agreement. When you select a language, the SLA will be displayed.

When you are finished examining the SLA, select **1** if you wish to accept the terms.

If you accept the SLA, the DMC login prompt will appear.

Log In to the DMC

CLI access is controlled through the use of a login name and password. Once you are connected to the DMC, you are prompted to enter a login name and password. The default log-in user name and password are as follows:

Default user name: `admin`

Default password: `admin`

It is recommended that you change all default system password after initial configuration and as regularly as required under your network security policies.

Enter Global Configuration Mode

The DMC uses a rich CLI command set with multiple command modes. For an overview of CLI modes and features, see "Command Basics" on page 71. The remainder of this chapter will display all commands necessary for initial configuration, but only those command relevant to the specific configuration tasks will be called into example.

After logging in, perform the following commands to enter the CLI Global Configuration mode:

```
DMC> enable
DMC# configure terminal
DMC(config)#
```

The `enable` command initiates Privileged EXEC mode, and the `configure terminal` command readies the DMC for basic configuration.

Configure the DMC IPv4 Addresses (Optional)

Each DMC must have IPv4 connectivity to the VMware vCenter, as well as to the hosts that will participate in the SDN VE system.

By default, the DMC is enabled for dynamic IPv4 addressing using DHCP. If there is a DHCP server available in your network, the DMC will automatically acquire IPv4 address, gateway, and DNS configuration. If using DHCP, you can skip static address configuration.

However, if DHCP is not available in your network or if you wish to override DHCP and configure static IPv4 addresses for the DMC, enter the following commands, depending on whether you prefer IPv4 address/netmask or CIDR notation.

Using IPv4 Address and Netmask

The following steps use IPv4 dotted-decimal (*a*`.`*b*`.`*c*`.`*d*) notation.

1. Set the DMC address:

```
DOVE(config)# system ipmgmt set ip addr <DMC IPv4 address> mask <netmask>
```

where *DMC IPv4 address* is the IPv4 address of the DMC, followed by the network *netmask* used for creating an address range.

2. Optional. Set a gateway (router/next-hop) address:

```
DOVE(config)# system nexthop set ip addr <gateway address> mask <netmask>
```

3. Optional. If necessary, add static DNS addresses:

```
DOVE(config)# system dns add ip addr <nameserver address> mask <netmask>
```

Using CIDR Notation

The following steps use CIDR dotted-decimal (*a.b.c.d/e*) notation.

1. Set the DMC address:

```
DOVE(config)# system ipmgmt set cidr <DMC address>
```

   where *DMC address* is the address of the DMC in CIDR notation.

2. Optional. Set a gateway (router/next-hop) address:

```
DOVE(config)# system nexthop set cidr <gateway address>
```

3. Optional. If necessary, add static DNS addresses:

```
DOVE(config)# system dns add cidr <nameserver address>
```

Using DHCP

DHCP if used by default. However, if you have configured static IPv4 addresses and prefer to return to DHCP operation, enter the following command:

```
DOVE(config)# system ipmgmt set dhcp
```

Note: Switching to DHCP will clear the static IPv4 addresses for the DMC and its gateway, DNS, and high-availability configuration.

Verifying Addresses

You can verify DMC IPv4 address and gateway configuration using the `show ipmgmt` command.

You can verify DNS settings using the `show dns` command.

Establish DMC High-Availability

As noted in the preceding installation process, two DMC modules on different hosts are required for high-availability (HA). HA provides resilience in the event that the active DMC fails. When HA is established, all configuration is performed via the primary DMC and is automatically synchronized with the secondary DMC, which will take over as the active DMC if the primary fails.

Configure the HA External IPv4 Address

On the primary DMC module, configure an external IPv4 address that will be used for master access to the DMC HA cluster as a whole. The address can be configured by IPv4 address and netmask or CIDR designation using one of the following Global Configuration mode commands:

- `system ha external set ip ip` *<IPv4 address>* `[mask` *<netmask>*`]`
- `system ha external set cidr` *<CIDR>*

For example:

```
DOVE(config)# system ha external set ip ip 9.70.27.245
```

Verify the setting with the `show ha-external` command.

Configure the HA Peer IPv4 Address

If necessary, access the secondary DMC module's CLI to obtain the secondary's IPv4 address using the `show ipmgmt` command. For example:

```
DMC(config)# show ipmgmt
Manage IP Info
============================================================
      Method:                                        Dynamic
          IP:                                     9.70.27.25
        MASK:                                  255.255.255.0
     NETXHOP:                                    9.70.27.254
         DNS:                                     9.0.130.50
                                                  9.0.128.50
```

Then, on the primary DMC, register the IPv4 address of the secondary DMC module. The address can be configured by IPv4 address and netmask or CIDR designation using one of the following Global Configuration mode commands:

- `system ha peer set ip ip` *<IPv4 address>* `[netmask` *<netmask>*`]`
- `system ha peer set cidr` *<CIDR>*

For example, on the primary DMC, the secondary DMC IPv4 address is used:

```
DMC(config)# system ha peer set ip ip 9.70.27.25 netmask 255.255.255.0
```

The primary DMC will automatically configure the secondary DMC with the proper HA external address and HA peer information and both modules will restart in hot standby mode (HSB), with both set to secondary mode.

Once the modules are restarted, the peer address on either module may be verified with the `show ha-peer` command.

Promote the Primary DMC Module

In the primary DMC CLI, set the module to act in primary mode:

```
DMC(config)# system ha type set type primary
```

The primary DMC module will automatically configure its peer as a secondary. It will also start the process of synchronizing the primary DMC configuration on to the secondary module. The synchronization is performed in a background process, and completion time depends on the complexity of the primary DMC configuration.

Check the HA synchronization status with the show ha-synchronization command. The output will show the process as `Synchronizing` (in progress) or `Synchronized` (complete)

Start the HA Engine

Once the HA synchronization process is complete, the HA feature can be started. Use the following command:

```
DMC(config)# system ha start
```

The HA sequence is performed in a background process. The "`HA started`" message will be displayed on the console when complete.

Use the `show ha` command to examine the HA status.

The Browser-Based Interface

Although this *User Guide* focuses on use of the CLI, most of the common configuration, management and operation features of the SDN VE can be accessed via the built-in Browser-Based Interface (BBI) using a standard Web browser.

The BBI supports HTTPS on default port 443 and is available once initial configuration of DMC HA is complete. To access the BBI, enter the following URL into your browser:

`https://`*<DMC HA external IPv4 address>*

Note: Be sure to use the HA external IPv4 address for the DMC cluster, and not the individual primary or secondary DMC IPv4 address. This helps ensure connection in case the primary DMC fails.

Next Steps

Once high-availability is operating on the DMC cluster, a minimum of five DSA modules must be installed and initialized as covered in the next chapter.

Chapter 3. Installing DSA Modules

After the DOVE Management Console (DMC) is installed as described in the previous chapter, the DOVE Service Appliance (DSA) modules must be installed.

DSA modules are versatile software modules capable of being differentiated after installation to provide one of two vital functions in the SDN VE system:

- DOVE Connectivity Service (DCS)

  Each DCS contains network information pertaining to nearby VMs, gateways and virtual switches in the SDN VE system. Domain information is synchronized among partner modules to provide distributed virtual networking capabilities.

  A minimum of two (2) DCS modules (installed on different hosts) are required for high-availability (HA) resilience. Three (3) are recommended.

- DOVE Gateway (DGW)

  Each DGW can serve as a connection to an external, non-virtual network.

  – External Gateways are associated with a specific port in the physical network.

  – VLAN Gateways are associated with legacy VLAN broadcast domains.

  A minimum of two (2) DGW modules (installed on different hosts) are required for HA resilience.

The remainder of this chapter describes installing and initializing the DSA modules required for HA resilience.

Deploying the DSA Software

Though deploying DSA software can be accomplished using either the VMware vSphere Client, vSphere Web Client, or OVF Tool, the procedure shown in this *User Guide* depicts only the vSphere Client. If using one of the other tools, extrapolate from the information provided.

Follow these steps to deploy and start the required DSA modules:

1. Download the DSA OVA file from IBM.
2. Place the OVA file on a system that has access to the VMware vSphere Client (such as an administrative laptop).

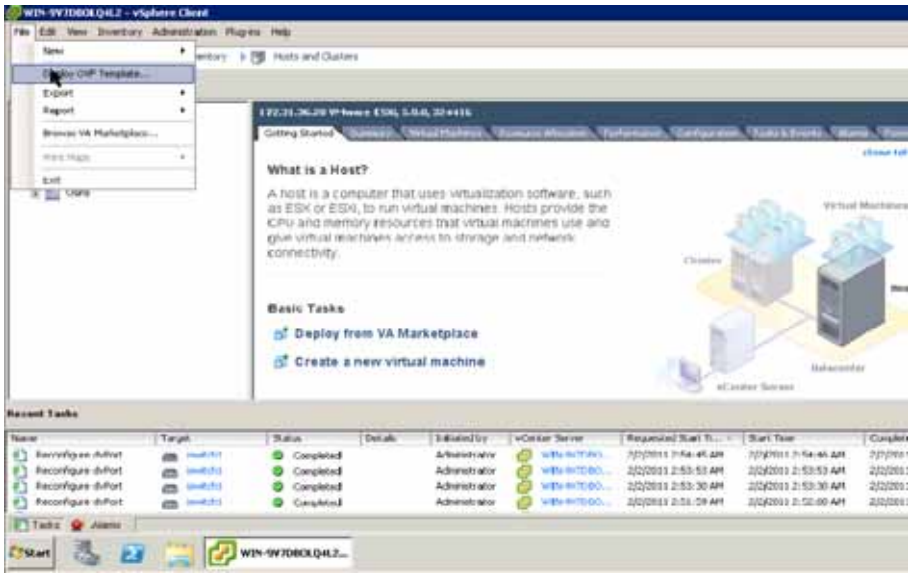
Note: At least four DSA modules are required for high-availability resilience: A minimum of two (installed on different hosts) for DCS modules, and a minimum of two (installed on different hosts) for DGW modules. More can be installed if desired. Perform the remaining steps once for each module.

3. Select an ESX host on which to deploy the DSA.

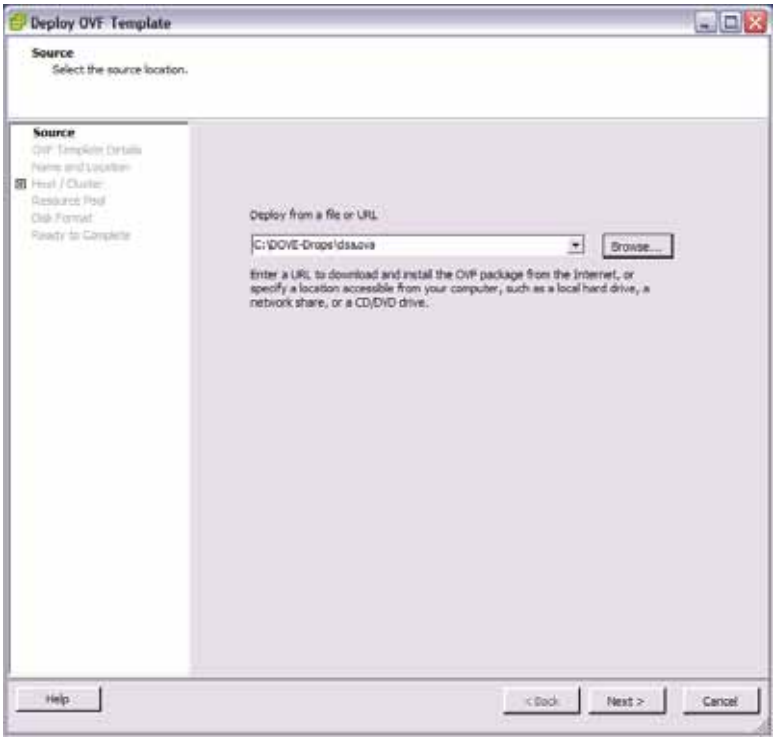
   Each DSA is required to have Layer 3 connectivity to the designated vCenter and participating DMC modules.

4. Launch the VMware vSphere Client and connect either to the vCenter that manages the host where the DSA will be deployed or directly to the ESX host.

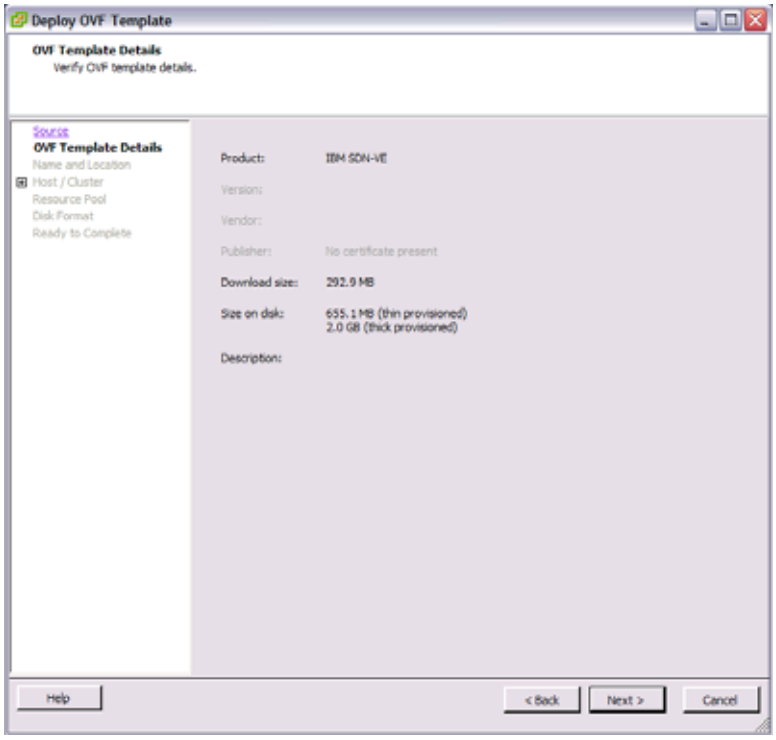
5. From the vSphere Client, select the target ESX host and choose **File > Deploy OVF Template** as shown below:



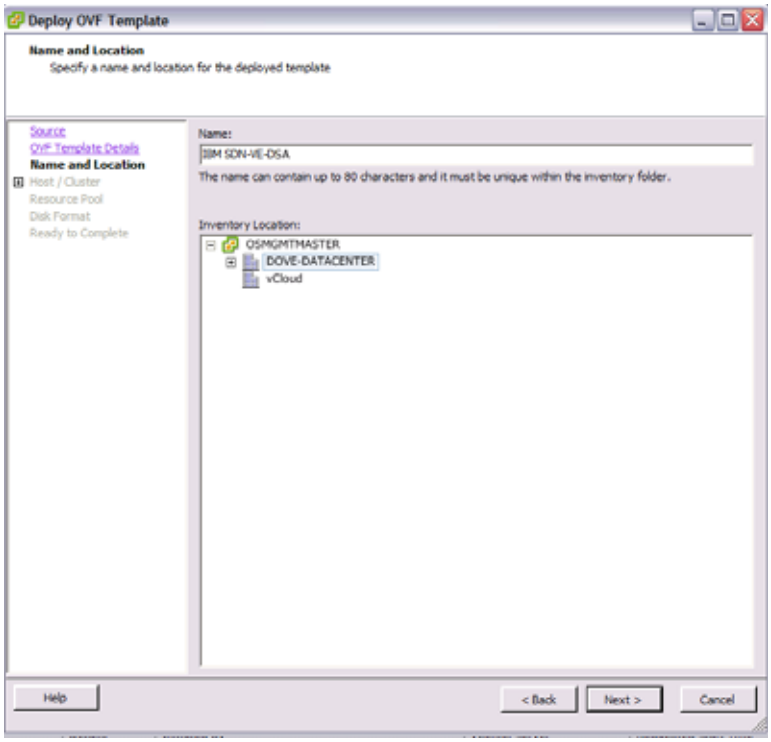
6. Select the location where the OVA file is stored and click **Next**.



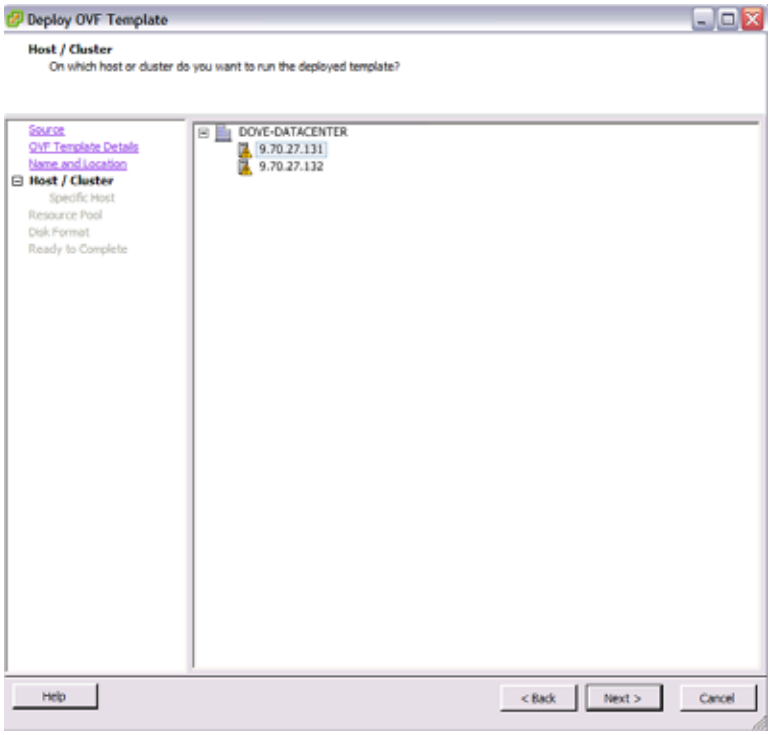
7. Verify the OVA details and click **Next**.



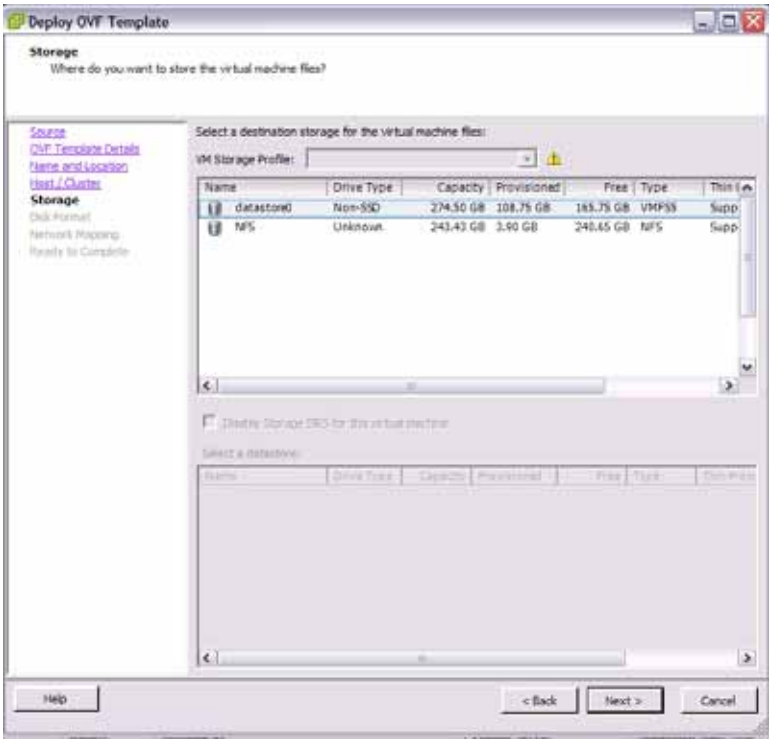
8. Provide a name for the DSA module and click Next.



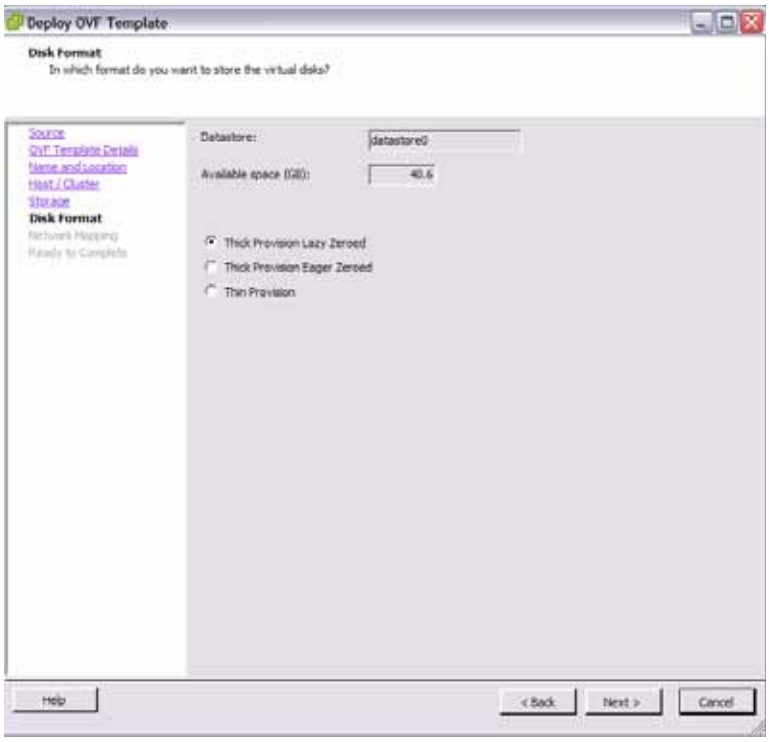
9. Specify the host or cluster on which to deploy the DSA and click **Next**.



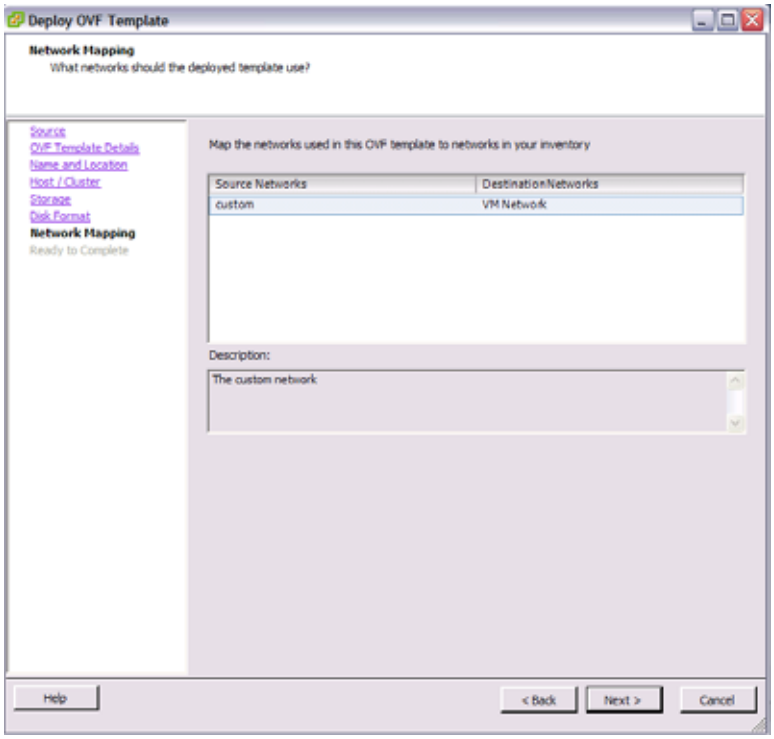
10. Specify a location on the VM where DSA files should be stored, and click **Next**.



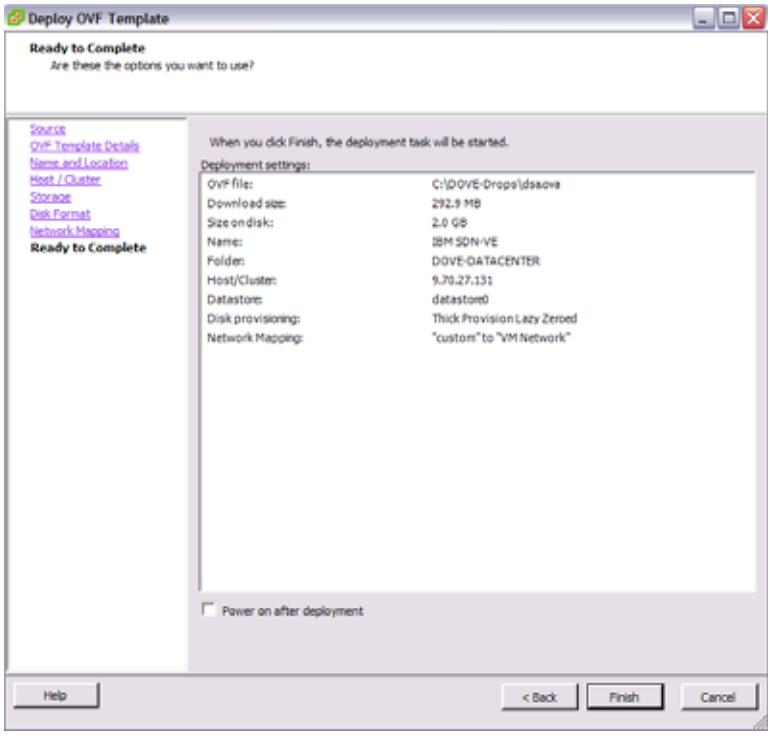
11. Select a disk format and click **Next**. The recommended format is Thick Provisioned Lazy Zeroed.



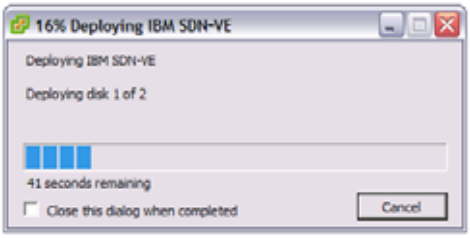
12. Map the network for DSA controller use and click **Next**.



13. Verify the specified options, select the “Power on after deployment” option, and click **Next**.



This will initiate the DSA module VM deployment:



The DSA VM will power on when deployment is complete, and the DSA console will appear.

Initial DSA Setup

A minimum of five DSA modules are required. After installing the DSA modules on VM hosts, each DSA must be manually configured by entering commands into the built-in Command-Line Interface (CLI). Initially, the CLI can be accessed only through each DSA VM console on the vSphere Client. Later, if desired, the CLI can be accessed via remote SSH connection.

Note: Configuration of the DSA must be performed solely from the DSA console, and not through the vCenter interface (even in cases where the vCenter interface seems to allow it). However, host operations (such as adding ESX hosts and uplinks or assigning VM network interfaces to vDS ports or profiles) must be done through the vCenter interface.

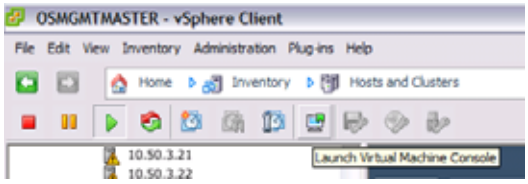
Perform the following initial DSA setup for all DSA modules.

Start the DSA Module

When following the provided installation instructions, the DSA module automatically starts when the VM is powered on.

However, to manually access the console under other conditions, use the following procedure:

1. Log-in to the VMware vCenter via your vSphere Client.
2. Right-click on the target DSA VM and select the option to “Open Console.” Alternately, you can click on the Console icon.



The VM console for the selected DSA will appear.

Examine the License Agreement

The first time the DSA is started, you will be prompted to read the Software Licence Agreement. When you select a language, the SLA will be displayed.

When finished examining the SLA, select **1** if you wish to accept the terms.

If you accept the SLA, the DSA login prompt will appear.

Log In to the DSA

CLI access is controlled through the use of a login name and password. Once you are connected to the DSA, you are prompted to enter a login name and password. The default log-in user name and password are as follows:

Default user name: `admin`

Default password: `admin`

It is recommended that you change all default system password after initial configuration and as regularly as required under your network security policies.

Enter Global Configuration Mode

The DSA uses a CLI command set with multiple command modes. For an overview of CLI modes and features, see “Command Basics” on page 71. The remainder of this chapter will display all commands necessary for initial configuration, but only those command relevant to the specific configuration tasks will be called into example.

After logging in, perform the following commands to enter the CLI Global Configuration mode:

```
DSA> enable
DSA# configure terminal
DSA(config)#
```

The `enable` command initiates Privileged EXEC mode, and the `configure terminal` command readies the DSA for basic configuration.

Configure the DSA IPv4 Address (Optional)

Each DSA must have IPv4 connectivity to the VMware vCenter, as well as to the DMC modules that will participate in the SDN VE system.

By default, the DSA is enabled for dynamic IPv4 addressing using DHCP. If there is a DHCP server available in your network, the DSA will automatically acquire IPv4 address, gateway, and DNS configuration. If using DHCP, you can skip static address configuration.

However, if DHCP is not available in your network or if you wish to override DHCP and configure static IPv4 addresses for the DSA, enter one of the following commands, depending on whether you prefer IPv4 address/netmask or CIDR notation:

- `ipmgmt set ip addr` *<DSA IPv4 address>* `mask` *<netmask>*

  where *DSA IPv4 address* is the IPv4 address of the DSA, followed by the network *netmask* used for creating an address range.
- `ipmgmt set ip cidr` *<DSA CIDR address>*

  where *DSA CIDR address* is the address of the DSA in CIDR notation.

You can verify DSA IPv4 address using the `show ipmgmt` command.

Using DHCP

DHCP if used by default. However, if you have configured static IPv4 addresses and prefer to return to DHCP operation, enter the following command:

```
DSA(config)# ipmgmt set dhcp
```

Note: Switching to DHCP will clear the static IPv4 addresses for the DSA.

Attach to the DMC Cluster IPv4 Address

All DSA modules get the remainder of their functional configuration through the active DMC operating at the DMC cluster's HA external IPv4 address.

Use the DSA CLI to attach the DSA to the DMC cluster. For each DSA, specify the DMC cluster address (see "Configure the HA External IPv4 Address" on page 31) using the following Global Configuration command:

```
DSA(config)# dmc set ip addr <DMC HA external IPv4 address>
```

Note: Be sure to use the HA external IPv4 address for the DMC cluster, and not the individual primary or secondary DMC IPv4 address. This helps preserve DSA communication resilience to the DMC cluster in case the primary DMC fails.

To verify DSA to DMC connectivity, use the DMC CLI `show service-appliance` command:

```
DMC# show service-appliance

DCS Service Appliances:
   ID         IP      SERVICE     ROLE      AGE_TIME   CONFIG      BUILT
                     CAPABILITY   ASSIGNED             VERSION   VERSION
  ================================================================================
    1     9.70.27.54        CS        N        13 s    0/   1   1.0.0.130530
    2    9.70.27.155        CS        N        15 s    0/   1   1.0.0.130530
    3    9.70.27.145        CS        N        11 s    0/   1   1.0.0.130530
    4    9.70.27.160        CS        N        12 s    0/   1   1.0.0.130530

GW Service Appliances:
   ID         IP      SERVICE     ROLE      AGE_TIME   CONFIG      BUILT
                     CAPABILITY   ASSIGNED             VERSION   VERSION
  ================================================================
    1     9.70.27.54        GW        N         7 s    0/   1   1.0.0.130530
    2    9.70.27.155        GW        N        15 s    0/   1   1.0.0.130530
    3    9.70.27.145        GW        N         0 s    0/   1   1.0.0.130530
    4    9.70.27.160        GW        N        15 s    0/   1   1.0.0.130530
```

Note: Each of the installed DSA modules is shown in both the DCS list and the DGW list, but their roles as DCS or DGW is not yet assigned (`ROLE ASSIGNED = N`).

Specify DSA Roles

You can set each DSA to operate in either a DCS role or a DGW role. These roles are mutually exclusive: At any given time, the DSA can operate in one or the other, but not both. Roles are defined using the DMC CLI (not via the DSA itself).

On the DMC, assign DCS roles to at least two unassigned modules (on different hosts) using the following Global Configuration mode command:

`service set-dcs-role ids` *<list of target DSA modules>*

where the list is a comma separated list of numeric DSA IDs as seen in the `show service-appliance` command (see page 41).

Also assign DGW roles for two unassigned modules (on different hosts) using the similar command:

`service set-dgw-role ids` *<list of target DSA modules>*

For example:

```
DMC(config)# set-dcs-role ids 1,2
DMC(config)# set-dgw-role ids 3,4
```

Verify the settings using the `show service-appliance` command:

```
DMC(config)# show service-appliance

DCS Service Appliances:
   ID         IP      SERVICE     ROLE      AGE_TIME   CONFIG      BUILT
                     CAPABILITY   ASSIGNED             VERSION   VERSION
  ================================================================================
    1     9.70.27.54        CS        Y        13 s    0/   1   1.0.0.130530
    2    9.70.27.155        CS        Y        15 s    0/   1   1.0.0.130530
    3    9.70.27.145        CS        N        11 s    0/   1   1.0.0.130530
    4    9.70.27.160        CS        N        12 s    0/   1   1.0.0.130530

GW Service Appliances:
   ID         IP      SERVICE     ROLE      AGE_TIME   CONFIG      BUILT
                     CAPABILITY   ASSIGNED             VERSION   VERSION
  ================================================================
    1     9.70.27.54        GW        N         7 s    0/   1   1.0.0.130530
    2    9.70.27.155        GW        N        15 s    0/   1   1.0.0.130530
    3    9.70.27.145        GW        Y         0 s    0/   1   1.0.0.130530
    4    9.70.27.160        GW        Y        15 s    0/   1   1.0.0.130530
```

Once roles are successfully set, the "ROLE ASSIGNED" field will be Y (Yes) in the appropriate role table.

Next Steps

Once DSA roles have been assigned for all required modules, a DS 5000V virtual switch must be installed and initialized as covered in the next chapter.

Chapter 4. Installing the DS 5000V

The IBM System Networking DS 5000V (5000V), version 1.1, is a virtual distributed switch (vDS) solution for VMware. It provides network switching within the SDN VE network fabric.

This chapter describes installing the 5000V as part of the SDN VE solution. These steps vary from those stated in the 5000V User Guide, which covers installing the 5000V as a stand-alone vDS (without SDN VE).

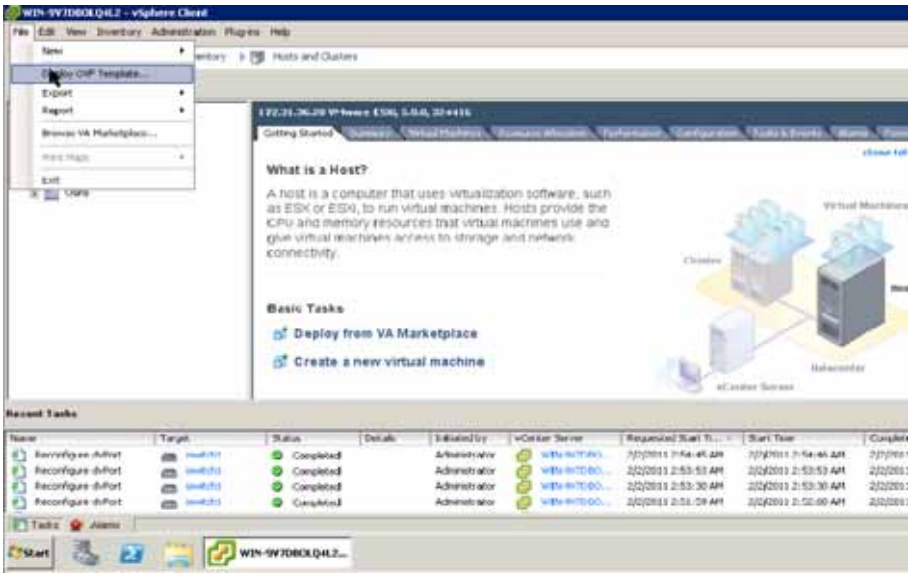
Deploying the 5000V Controller Software

Though deploying 5000V controller software can be accomplished using either the VMware vSphere Client, vSphere Web Client, or OVF Tool, the procedure shown in this *User Guide* depicts only the vSphere Client. If using one of the other tools, extrapolate from the information provided.

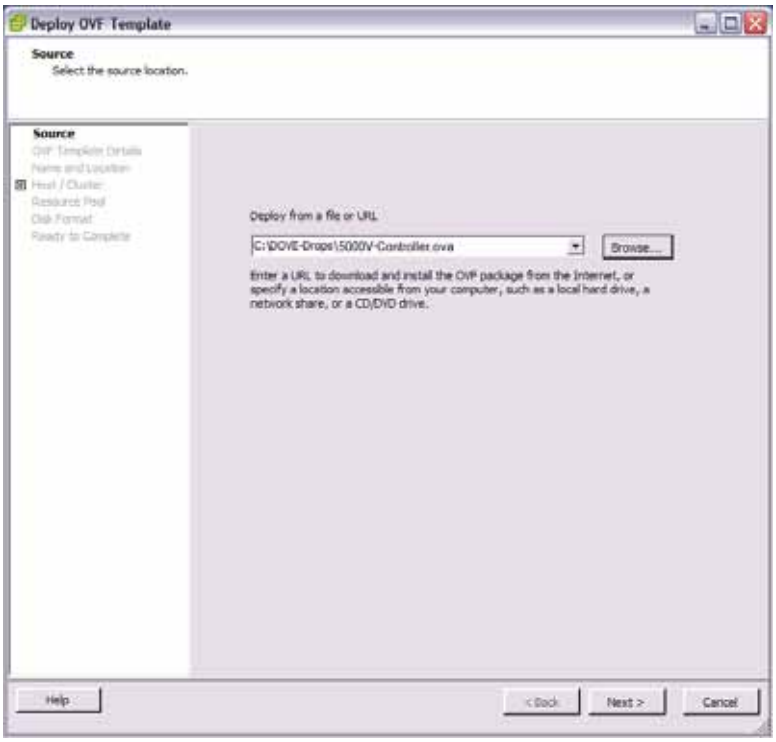
Follow these steps to deploy and start the required 5000V controller software:

1. Download the 5000V version 1.1 controller OVA file from IBM.
2. Place the OVA file on a system that has access to the VMware vSphere Client (such as an administrative laptop).
3. Specify an ESX host on which to deploy the controller.

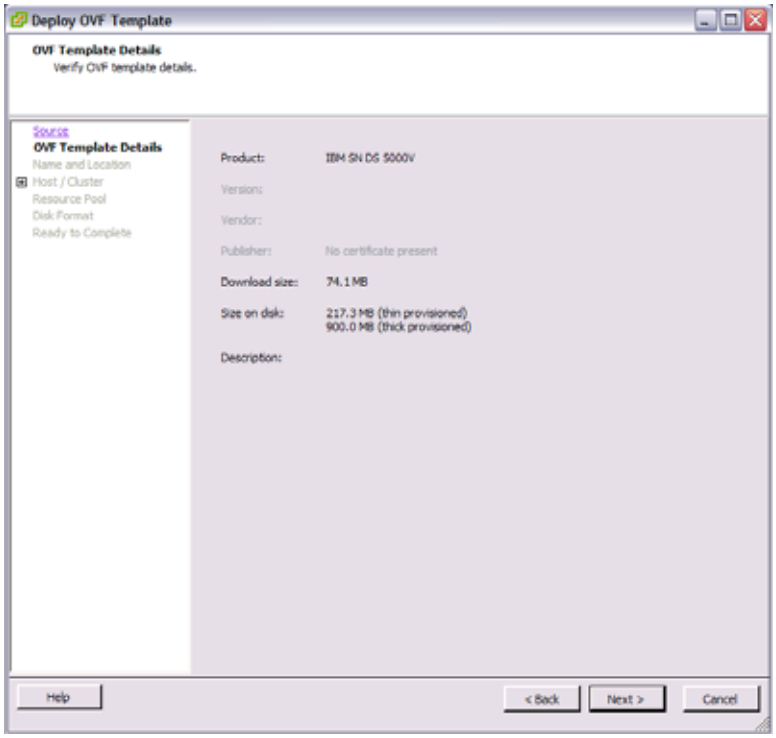
   The controller host merely provides an environment in which the 5000V controller appliance will run. It is not required to participate as a vDS host and may be a different class of device than those where the vDS host modules will later be installed. The primary requirement is for the controller host to have Layer 3 connectivity to the designated vCenter and the SDN VE DMC cluster.
4. Launch the VMware vSphere Client and connect either to the vCenter that manages the host where the 5000V controller will be deployed or directly to the ESX host.
5. From the vSphere Client, select the target ESX host and choose **File > Deploy OVF Template** as shown below:



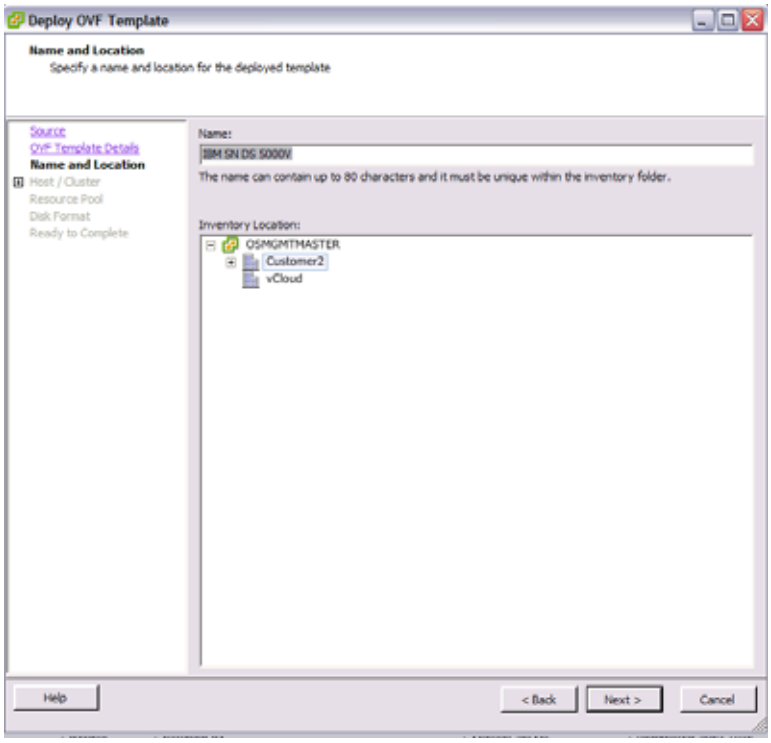
6. Select the location where the OVA file is stored and click **Next**.



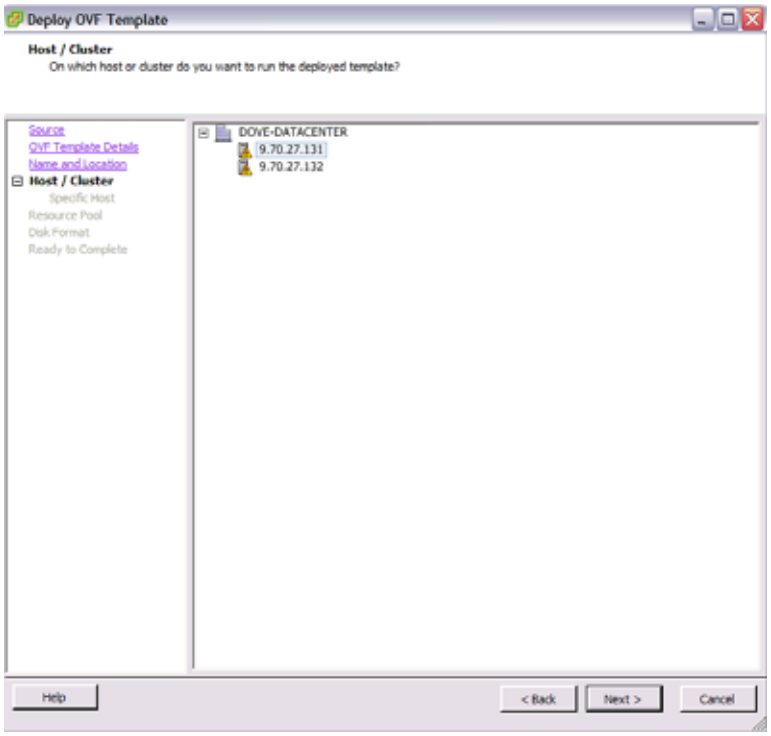
7. Verify the OVA details and click **Next**.



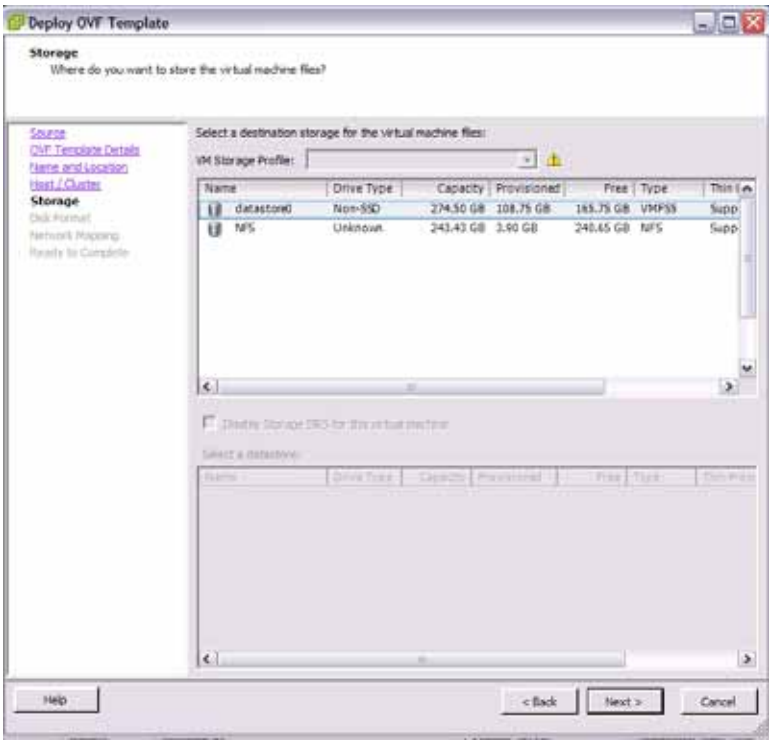
8. Provide a name the 5000V controller and click Next.



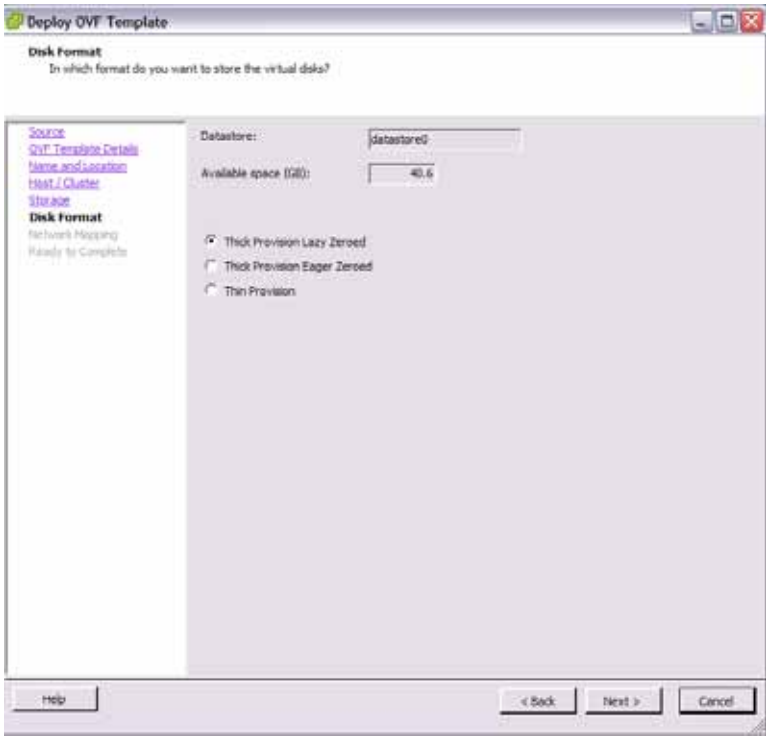
9. Specify the host or cluster on which to deploy the 5000V controller and click **Next**.



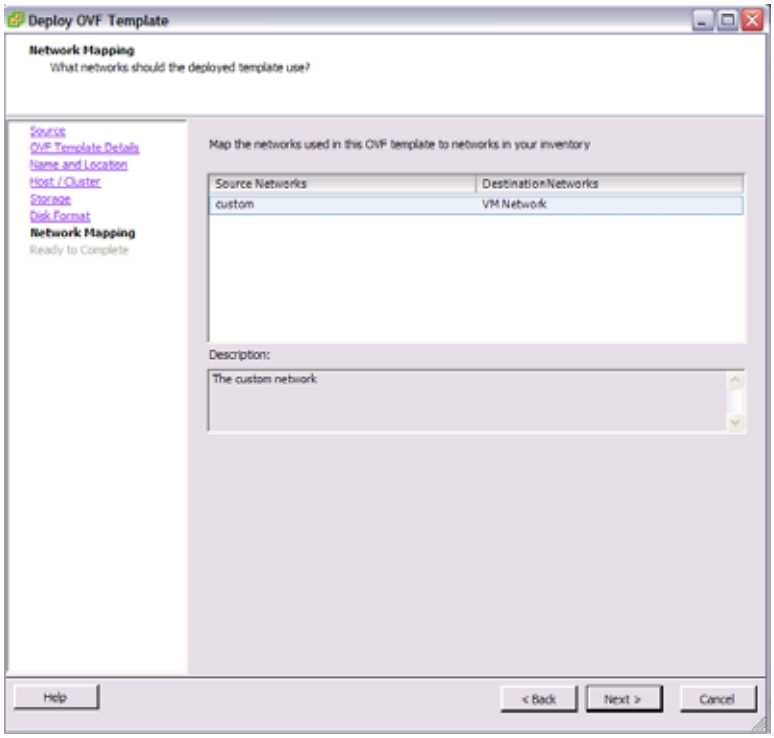
10. Specify a location on the VM where 5000V controller files should be stored, and click **Next**.



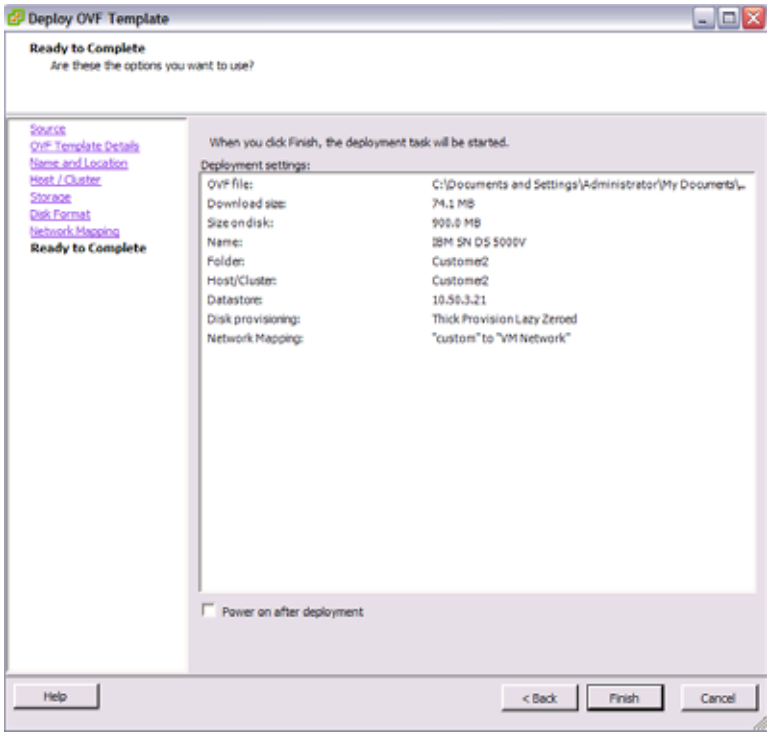
11. Select a disk format and click **Next**. The recommended format is Thick Provisioned Lazy Zeroed.



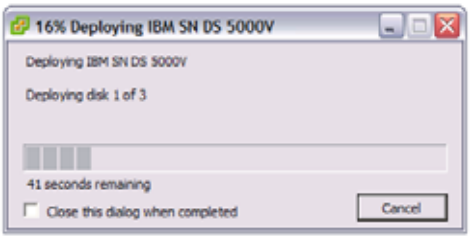
12. Map the network for 5000V controller use and click **Next**.



13. Verify the specified options, select the “Power on after deployment” option, and click **Next**.



This will initiate the 5000V controller VM deployment:



The 5000V controller VM will power on when deployment is complete, and the controller VM console will appear.

Initial 5000V Controller Setup

The 5000V must be manually configured by entering commands into the controller's built-in Command-Line Interface (CLI). Initially, the CLI can be accessed only through the 5000V controller VM console on the vSphere Client. Later, if desired, the CLI can be accessed via remote Telnet or SSH connections.

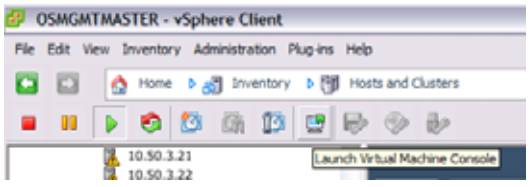
Note: Configuration of the 5000V vDS must be performed solely from the 5000V CLI, and not through the vCenter interface (even in cases where the vCenter interface seems to allow it). However, host operations (such as adding ESX hosts and uplinks or assigning VM network interfaces to vDS ports or profiles) must be done through the vCenter interface.

Starting the 5000V Controller

When following the provided installation instructions (see Step 13 on page 47), the controller console automatically appears when the 5000V controller VM is powered on.

However, to manually access the controller console under other conditions, use the following procedure:

1. Log-in to the VMware vCenter via your vSphere Client.
2. Right-click on the 5000V controller VM and select the option to "Open Console." Alternately, you can click on the Console icon.



The VM console for the 5000V controller will appear.

Examine the License Agreement

The first time the 5000V controller is started, you will be prompted to read the Software Licence Agreement. When you select a language, the SLA will be displayed.

When you are finished examining the SLA, select **1** if you wish to accept the terms.

If you accept the SLA, the 5000V controller login prompt will appear.

Log In to the 5000V Controller

CLI access is controlled through the use of a login name and password. Once you are connected to the 5000V controller, you are prompted to enter a login name and password. The default log-in user name and password are as follows:

Default user name: `admin`

Default password: `admin`

It is recommended that you change all default system password after initial configuration and as regularly as required under your network security policies.

Enter Global Configuration Mode

The 5000V controller uses a rich CLI command set with multiple command modes. For an overview of CLI modes and features, refer to the *Distributed Switch 5000V User Guide.* The remainder of this chapter will display all commands necessary for initial configuration, but only those command relevant to the specific configuration tasks will be called into example.

After logging in, perform the following commands to enter the CLI Global Configuration mode:

```
5000V> ena
5000V# configure terminal
5000V(config)#
```

The `ena` command initiates executive privilege mode, and the `configure terminal` command readies the controller for configuration.

Verify the 5000V Controller Version

The SDN VE solution requires version 1.1 of the DS 5000V. To verify the correct version of software has been deployed, use the following command:

```
5000V(config)# show running-config
```

Near the top of the output, a "`Software Version`" message is displayed. Verify that the version number is `1.1.0` or higher.

If an earlier version is deployed, refer to "Updating the Switch Software Image" in the "Boot Options" chapter in the *Distributed Switch 5000V User Guide.*

Configure the 5000V IPv4 Addresses (Optional)

The 5000V controller must have IPv4 connectivity to the VMware vCenter, as well as the hosts that will participate in the SDN VE system.

By default, the 5000V controller is enabled for dynamic IPv4 addressing using DHCP. If there is a DHCP server available in your network, the controller will automatically acquire its IPv4 address and gateway configuration. If using DHCP, you can skip static address configuration.

However, if DHCP is not available in your network or if you wish to override DHCP and configure static IPv4 addresses for the 5000V controller, enter the following command:

```
5000V(config)# interface ip-mgmt address <IPv4 address> [<mask>]
```

where *IPv4 address* is the address of the controller in dotted-decimal notation, optionally followed by the network *mask* used for creating an address range

If desired, you can also configure the *gateway* IPv4 address that the controller should use for outbound traffic:

```
5000V(config)# interface ip-mgmt gateway <gateway IPv4 address>
5000V(config)# interface ip-mgmt gateway enable
```

Create the Global vDS Instance

The 5000V controller must be associated with a virtual distributed switch (vDS) for a particular virtual data center. The following CLI commands on the controller VM console are used to create the required association to the vCenter:

```
5000V(config)# iswitch vcenter <vCenter IPv4 address> <user name>
```

The *vCenter IPv4 address* represents the vCenter to which the 5000V will connect and *username* is the vCenter login name.

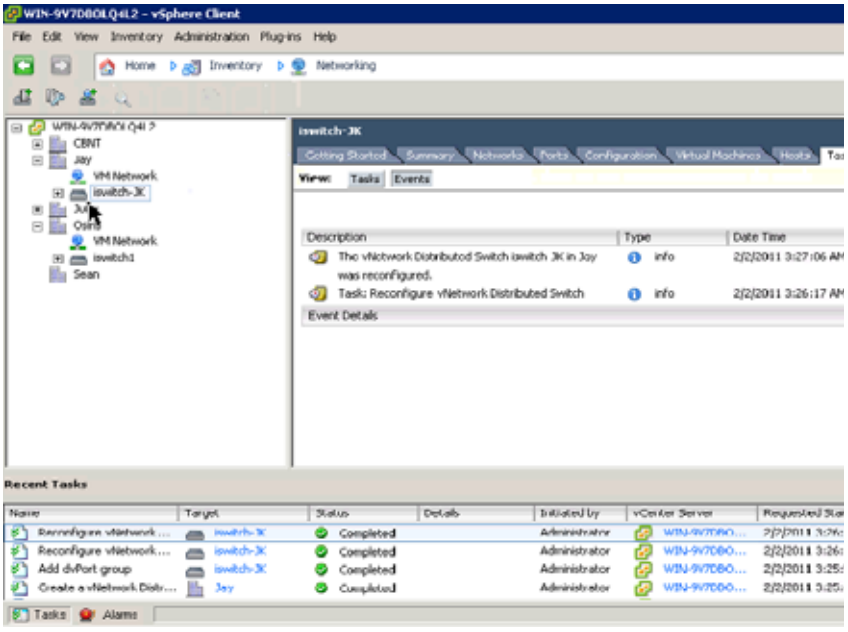
The system will then prompt you for the vCenter login password and its logical port number. By default, the vCenter operates on recommended TCP port number 443. However, if your vCenter communicates on a different port, enter the port number configured for the service.

Next, the 5000V controller must be associated with the vDS:

```
5000V(config)# iswitch vds <vDS name> <datacenter name>
```

Note: The assigned names cannot include internal spaces.

When this configuration is complete, the 5000V vDS will appear at the vCenter in the **Home > Inventory > Networking** view:



Note: Once the controller is associated a vDS in the vCenter, whenever the IPv4 address of the 5000V controller is changed (statically or via DHCP renewal), you must save the 5000V configuration and reload the controller in order to reestablish the required association.

Attach to the DMC Cluster IPv4 Address

The 5000V must coordinate its ongoing configuration with the active DMC. Use the 5000V CLI to select the DMC cluster's HA external IPv4 address (from "Configure the HA External IPv4 Address" on page 31). Specify the address using the following Global Configuration command:

```
5000V(config)# iswitch dmc <DMC HA external IPv4 address>
```

Note: Be sure to use the HA external IPv4 address for the DMC cluster, and not the individual primary or secondary DMC IPv4 address. This helps preserve 5000V communication with the DMC cluster in case the primary DMC fails.

Verify the DMC configuration using the `show running-config` command on the 5000V controller CLI and examining the `iswitch` output elements.

Also verify that a DOVE Tunnel End Point (TEP) profile has been automatically created at the vCenter.

Next Steps

Once installation and initial setup of the DMC, DSA, and 5000V elements are complete, the system is ready for virtual network configuration as discussed in the next chapter of this *User Guide*.

Chapter 5. Virtual Network Configuration

Overlay Configuration

Once basic installation and initial configuration is complete, the overlay network can be configured. The overlay network consists of domains, virtual networks, the address spaces that will be mapped to the networks, and the policies between networks. Overlay configuration is performed via the DMC.

Create Domains

Domains are created with the following Global Configuration command in the DMC CLI:

domain add [**name**] <*domain name*>

The existing domains are shown via the `show domain` command.

For example:

```
DMC(config)# domain add name Corp
DMC(config)# show domain
                                Active/Total
Domain_ID      Domain_Name       Networks    Status
=======================================================
        1             Corp        0/0        Active
```

Create Networks

To create networks, first set the domain context using the following Global Configuration command:

domain set <*domain-name*>

Within the Domain Configuraiton mode, networks can be created using the following command:

network add [**id**] <*virtual network ID*> [**name**] <*domain name*>

For example:

```
DMC(config)# domain set Corp
config:(domain)Corp# network add id 1 name Corp_HR
config:(domain)Corp# network add id 2 name Corp_SALES
```

Created networks can be viewed using the `show network` command:

```
config:(domain)Corp# show network
Network_ID                    Network_Name    Domain_Name   Status
=====================================================================
         1                        Corp_HR    Corp          Active
         2                      Corp_SALES    Corp          Active
```

Define the Address Space for Each Network

Create Subnets

Create subnets from the Domain Configuration context using the following command:

subnet add [**net**] <*net*> [**mask**] <*mask*> [**nexthop**] <*nexthop*> [**type**] {**dedicated**|**shared**}

For example:

```
config:(domain)Corp# subnet add net 3.3.3.0 mask 255.255.255.0 nexthop
3.3.3.254 type dedicated
```

Created subnets are listed using the `show subnet` command:

```
config:(domain)Corp# show subnet

   ID        SUBNET(TYPE)           MASK        NEXTHOP        NETWORKS
================================================================================
    1          3.3.3.0(D)  255.255.255.0      3.3.3.254
    2          4.4.4.0(D)  255.255.255.0      4.4.4.254

   (S)  ====>  Shared Subnet
   (D)  ====>  Dedicated Subnet
```

Note: The *nexthop* IPv4 address should be the default route for all endpoints that attach to the network to which this subnet is bound.

Bind Subnets to the Networks

Because a subnet can be bound to multiple networks, it is necessary to configure bindings through the Network Configuration mode. This mode is accessed via the Domain Configuration mode, using the following command:

network set [**id**] <*network ID*>

where the network ID is as shown using the `show networks` command. Within the Network Configuration mode, you can bind the subnet to the current network context with the following command:

subnet index <*index*>

For example:

```
config:(domain)Corp# network set id 1
config:(domain)Corp:(network)1# subnet index 1
config:(domain)Corp:(network)1# exit
config:(domain)Corp# show subnet

   ID        SUBNET(TYPE)           MASK        NEXTHOP        NETWORKS
================================================================================
    1          3.3.3.0(D)  255.255.255.0      3.3.3.254                 1
    2          4.4.4.0(D)  255.255.255.0      4.4.4.254

   (S)  ====>  Shared Subnet
   (D)  ====>  Dedicated Subnet
```

Networks can contain subnets of only one type. The type that is added first determines what other subnets can be added to the network. So if a `dedicated` network was added first, all subsequent subnets that are added to that network need to be of type `dedicated`.

Define Policies

Policies are defines in the Domain Configuration mode using the following command:

policy add [**peers**] <*peers*> [**traffic-type**] <*traffic type*> [**action**] {**allow**|**deny**}

For example

```
config:(domain)Corp# policy add peers 1:2 traffic-type unicast action
allow
config:(domain)Corp# policy add peers 1:2 traffic-type multicast action
allow
```

Note: The peers are a colon-separated list of two virtual network IDs (VNIDs).

While policies act on a bi-directional basis, they are depicted in a unidirectional basis in the `show policy` command:

```
config:(domain)Corp# show policy
  SRC NETWORK    DST NETWORK        TRAFFIC_TYPE ACTION
============================================================
            1              2             unicast  allow
            2              1             unicast  allow
            1              2           multicast  allow
            2              1           multicast  allow
config:(domain)Corp# exit
DMC(config)#
```

Export Networks to the 5000V Controller

Before traffic can flow, you must export the created virtual networks to the 5000V controller. This makes the information available to the vDS for connected VMs.

To export a network, use the following Global Configuration command:

export [**Network_ID**] <*Network ID*> [**ip-addr**] <*IPv4 address*>

where <*Network ID*> is the VNID to be exported and <*IPv4 address*> is the IPv4 address of the 5000V controller (as shown in the `show interface ip-mgmt` command).

For example:

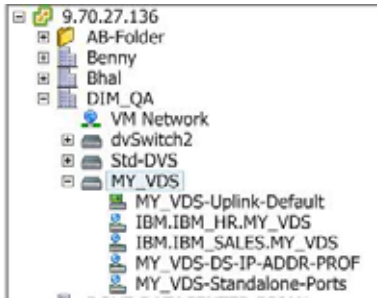
```
DMC(config)# export Network_ID 1 ip-addr 9.70.27.28
Please wait while the Network_ID is being exported
DMC(config)# export Network_ID 2 ip-addr 9.70.27.28
Please wait while the Network_ID is being exported
```

On the DS 5000V Controller console, messages will appear when the network profiles are created. For example:

```
Jun  4 2013 18:43:29 5000V:SYSTEM-INFO: Saved configuration to flash
successfully!

Jun  4 2013 18:43:29 5000V:SYSTEM-ALERT: Profile [IBM.IBM.HR.MY_VDS] got
created from DMC, config saved
```

To verify that the profiles have been created, use either vCenter or the 5000V controller show running-config command. For example:




```
5000V(config)# show running-config

Building configuration...
#
#switch-type “IBM System Networking Distributed Switch 5000V”
#Software Version 1.1.0.130603
#!!!!DO NOT EDIT ANYTHING ABOVE THIS LINE!!!!
#
!
!
iswitch vcenter 8.70.27.136 root 0x559b5fe219e61dec 443
iswitch vds MY_VDS DIM_QA dvs-9609 datacenter-1686
iswitch dmc 9.70.27.245
iswitch doveprof IBM.IBM_HR.MY_VDS 10 141 dvportgroup-9639
!
iswitch doveprof IBM.IBM_SALES.MY_VDS 10 151 dvportgroup-9640
!
!
!

!
iswitch doveprof IBM.IBM_HR.MY_VDS dvportgroup-9639
        vnid 1
iswitch doveprof IBM.IBM_SALES.MY_VDS dvportgroup-9640
        vnid 2
!

end
```

Network IDs that have been exported to a particular 5000V controller can be viewed at the DMC CLI with the command:

`show export-list [Remote-IP]` *<remote IPv4 address>*

For example

```
DMC(config)# show export-list Remote-IP 9.70.27.28
==============================
Remote-IP           Network_ID
==============================
8.70.27.28          1
8.70.27.28          2
```

Externalizing the Overlay Networks

To connect an overlay network to a traditional network, a gateway is used. There are two types of gateways: those that connect a virtual network to a legacy VLAN environment, and those that connect a virtual network to external hosts, including the Internet. A particular DSA assigned a role as a DOVE Gateway (DGW) can only function as one gateway type.

The first step in configuring any gateway is to select the gateway to be configured via the following command:

service gateway set [id] <*ID number*>

For example:

```
DMC(config)# show service-appliance

DCS Service Appliances:
   ID         IP      SERVICE     ROLE      AGE_TIME   CONFIG      BUILT
                     CAPABILITY   ASSIGNED             VERSION   VERSION
  ================================================================================
    1     9.70.27.54        CS        N        13 s    0/   1   1.0.0.130530
    2    9.70.27.155        CS        N        15 s    0/   1   1.0.0.130530
    3    9.70.27.145        CS        N        11 s    0/   1   1.0.0.130530
    4    9.70.27.160        CS        N        12 s    0/   1   1.0.0.130530

GW Service Appliances:
   ID         IP      SERVICE     ROLE      AGE_TIME   CONFIG      BUILT
                     CAPABILITY   ASSIGNED             VERSION   VERSION
  ================================================================
    1     9.70.27.54        GW        N         7 s    0/   1   1.0.0.130530
    2    9.70.27.155        GW        N        15 s    0/   1   1.0.0.130530
    3    9.70.27.145        GW        N         0 s    0/   1   1.0.0.130530
    4    9.70.27.160        GW        N        15 s    0/   1   1.0.0.130530
DMC(config)# service gateway set id 3
```

VLAN GW

Next, configure the tunnel endpoint's (TEP) IPv4 address with the following command:

ip-add [ip] <*addr*> **[mask]** <mask> **[nexthop]** <*nexthop*> **[type] dovetunnel [vlan]**

```
config:(gateway)3# ip-add ip 2.2.2.23 mask 255.255.255.0 nexthop
2.2.2.254 type dovetunnel vlan
```

After adding the TEP, change context to the network to be connected to the VLAN and use the following command:

vlan-gateway add [dgw_index] <*dgw_index*> **[vlan_id]** <*VLAN ID*>

```
config:(gateway)3# exit
DMC(config)# domain set Corp
config:(domain)Corp# network set id 1
config:(domain)Corp:(network)1# vlan-gateway add dgw_index 3 vlan_id 201
```

For example, this instructs the gateway shown in the service appliance list as index #3 (with a management IPv4 address of 9.70.27.145) to map traffic on virtual network 1 to VLAN ID 201

This completes the VLAN Gateway setup on the DMC.

Configure an External Gateway

When configuring an external gateway (EGW), after selecting the gateway index via the “service gateway set” command (see above), two IPv4 addresses need to be assigned to the gateway. The first is the TEP address of the gateway, assigned with the command:

ip-add [ip] <*addr*> **[mask]** <*mask*> **[nexthop]** <*nexthop*> **[type] dovetunnel [vlan]**

```
config:(gateway)4# ip-add ip 2.2.2.24 mask 255.255.255.0 nexthop
2.2.2.254 type dovetunnel vlan
```

The second is the external IPv4 address of the gateway, assigned with the command:

ip-add [ip] <*addr*> **[mask]** <*mask*> **[nexthop]** <*nexthop*> **[type] external [vlan]**

```
config:(gateway)4# ip-add ip 7.7.7.24 mask 255.255.255.0 nexthop
7.7.7.100 type external vlan
```

Once the IPv4 addresses are assigned, switch to the network context and use the command:

external-gateway add [dgw-index] <*dgw_index*> **[extip-range]** <*extip-range*> **[port-range]** <*port-range*>

```
config:(domain)Corp:(network)1# external-gateway add dgw-index 4
extip-range 7.7.7.25-7.7.7.26 port-range 8000-9000
WARNING: External IP Pool configuration in progress.
         May take several minutes to complete.
         Use ‘show ipv4-interfaces’ on gateway console to see IP list
```

This command sets up addresses 7.7.7.25 and 7.7.7.26 on gateway index #4 (with a management IPv4 address of 9.70.27.160) as NAT addresses for devices attached to VNID 1. Further, ports 8000-9000 will be used for outgoing connections.

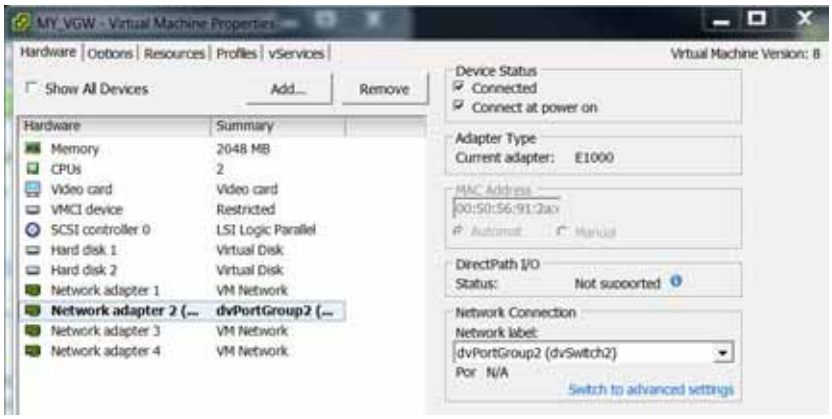
On the console of the DSA, these additional addresses can be verified using the `show ipv4-interfaces` command:

```
DSA(config)# show ipv4-interfaces
            0: 127.0.0.1
            1: 9.70.27.199
            2: 7.7.7.24
            3: 7.7.7.25
            4: 7.7.7.26
```

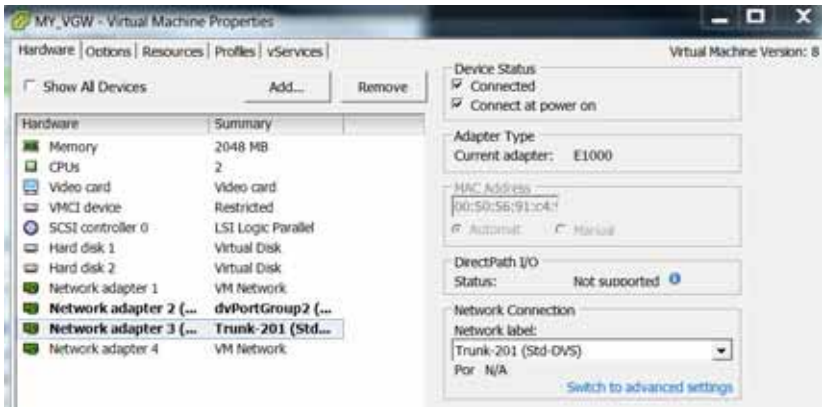
This completes the configuration of external gateways on the DMC.

Configuration of Gateway Interfaces

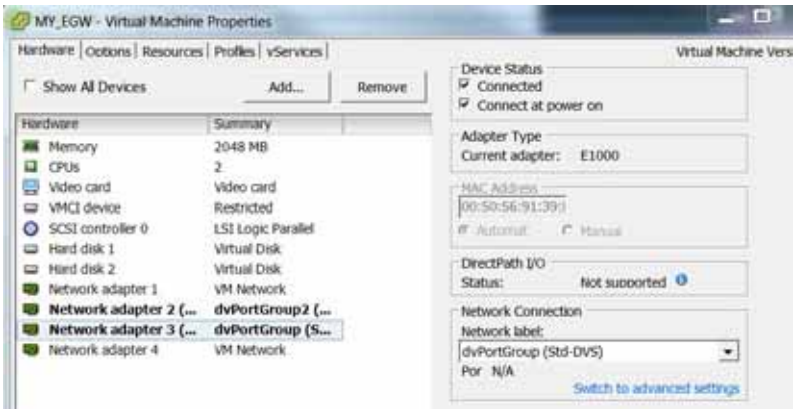
For connectivity to traditional networks, it is necessary to connect the VNICs of the service appliances that have a gateway role assigned to them so that they can communicate with the underlay network. From vCenter, right click on the appliance and select the “Edit Settings” menu item. Then select the hardware tab, and set one network adapter to the port group of the VDS.



For the VLAN gateway, we then need to select another vnic and set it to attach to the VLAN that it was configured with. To do this, select the pre-configured “tagged” profile that has been configured with the proper VLANID.



For the external gateway, the second vnic is attached via an untagged profile to a standard VDS that provides connectivity to the external network:



5000V Host Module

The 5000V vDS Host Module is deployed on ESXi hosts. It implements overlay networks support in addition to L2 switching required by VMs that wish to communicate via the SDN VE overlay networks.

Install 5000V Host Module

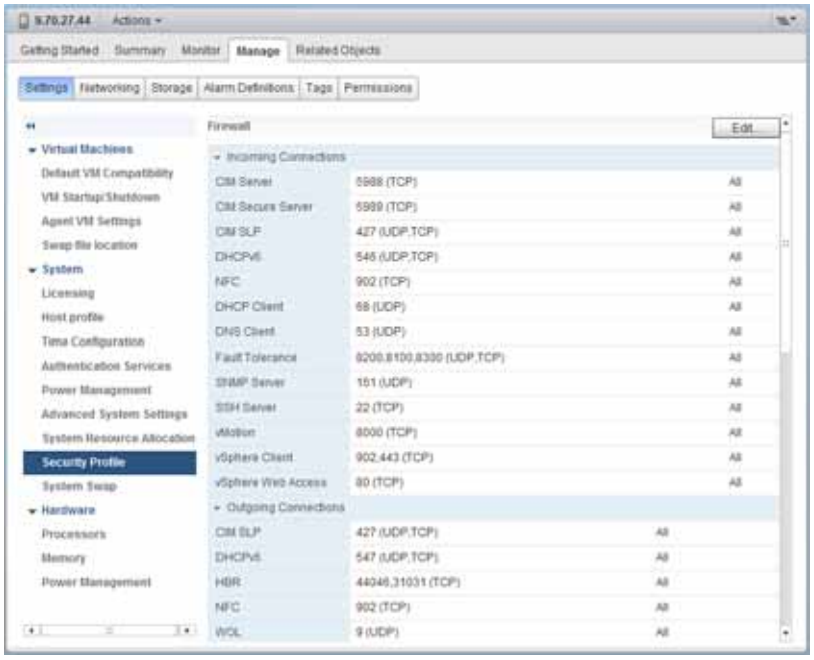
Preconditions

Verify ESXi Images

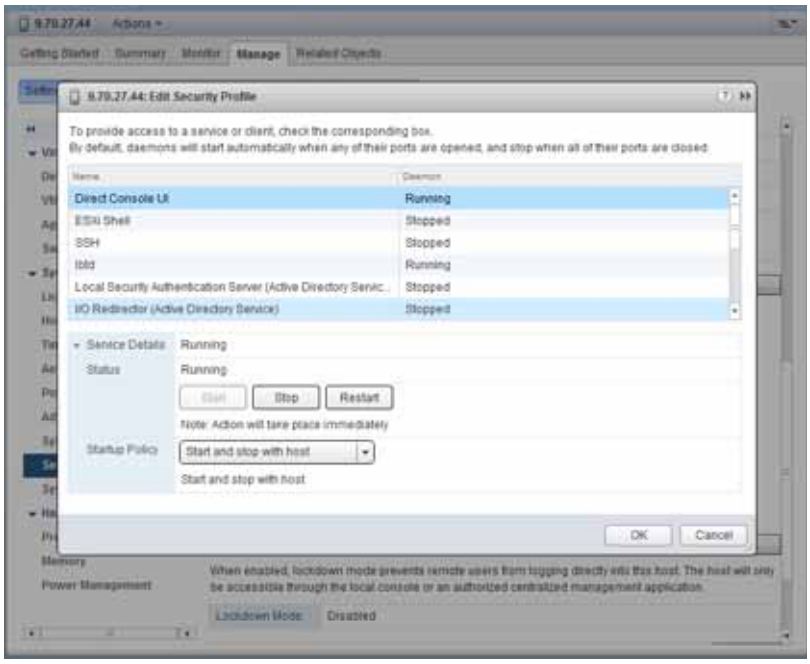
The ESXi hosts that will host the 5000V vDS Host Module must be running either VMware ESX 5.0 or 5.1 with test certificates.

Enable SSH on ESXi Hosts

To install the 5000V vDS Host Module, it is first necessary that the ESXi hosts be running ssh. To do this, go to vSphere, and select the Settings button under the Manage tab:



Scroll down to services and click the Edit button on the right.



Select ESXi Shell and SSH and start both of them, then click the OK button in the lower right. Verify by sshing to the ESXi host using the root and the ESXi root password.

Copy 5000V vDS Host Module File to ESXi Machines

Use `scp` to copy the OHM `zip` file to the destination ESXi machine:

```
[bhal@oc2072406814 Jun-03-2013]$ scp -p 5000V-host-module.zip
root@9.70.27.194:/tmp
Password:
5000V-host-module.zip
100%
```

Install 5000V vDS Host Module VIB

Use SSH to access the ESXi machine and log in as root. Then change to the directory where the zip file was copied.

Install the host module with the following command:

```
esxcli software vib install -d=file://`pwd`/5000V-host-module.zip
```

This will generate the following type of output:

```
/tmp # esxcli software vib install -d=file://`pwd`/5000V-host-module.zip
Installation Result
   Message: The update completed successfully, but the system needs to be
rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: IBM bootbank ibm-esx-5000V 1.1.0-130527
   VIBs Removed: IBM_bootbank_ibm-esx-5000V 1.1.0-130513
   VIBs Skipped:
```

When this is complete, reboot the ESXi host. After it reboots, re-enable the ESXi shell and SSH service (if necessary) and make sure that the host module is installed correctly:

```
esxcli software vib list | grep –ir 5000V
```

```
/tmp # esxcli software vib list | grep –ir 5000V
ibm-esx-5000V                1.1.0-130527                       IBM
VMwareAccepted 2013-5-31
```

Configure the Underlay (Physical) Networks at the DMC

Underlay network is the physical network to which the uplinks of 5000V vSwitches connect. This is the network over which SDN VE encapsulated packets flow between Tunnel End Points.

Since the vSwitches do not make use of the host's IPv4 routing capabilities, it is necessary to provide the IPv4 gateway information to the vSwitches. The vSwitches can learn the IPv4 address and Subnet that was configured for the VM Kernel NIC (vmknic) that was attached to the vSwitch. However, the Default Gateway information that is present for the host cannot be used by the vSwitches since the vSwitches may be connected to a physically separate and isolated network segment from the one in which the Default Gateway exists.

For this reason, it is necessary to configure the network segments to which the TEPs will connect and the Nexthop or Gateway IP that would perform IPv4 routing functions for that network segment.

Notes:

1. It is necessary to configure the network information on DMC ***before*** connecting vmknics to the vSwitches.
2. An underlay network configuration cannot be modified. To change the next hop, delete the net and mask combination (`underlay-network del` command) and add a new configuration.
3. Ensure that the TEPs (VMKNICs) are given addresses and netmasks that correspond to the configuration made on the DMC.
4. It is not necessary to configure the underlay network unless the TEPs span multiple subnets.

The commands are as follows:

- To configure an underlay network segment:

  `DMC(config)#` **`underlay-network add net 1.1.1.0 mask 255.255.255.0 nexthop 1.1.1.254`**

- To remove a previously configured network segment: (next hop cannot be specified)

  `DMC(config)#` **`underlay-network del net 1.1.1.0 mask 255.255.255.0`**

- To display the configured underlay networks:

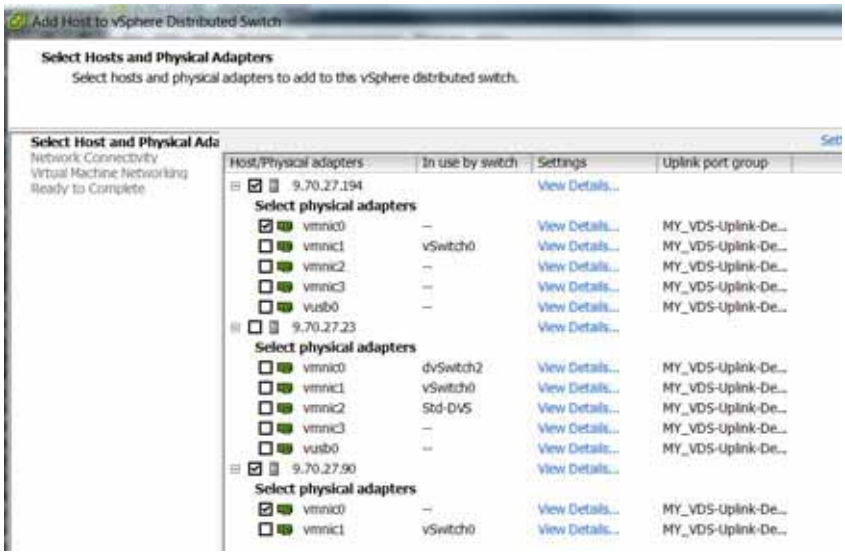
  `DMC(config)#` **`show underlay-network`**

  A sample output of this command:

```
            NET            MASK         NEXTHOP
=============================================
        1.1.1.0  255.255.255.0       1.1.1.254
```

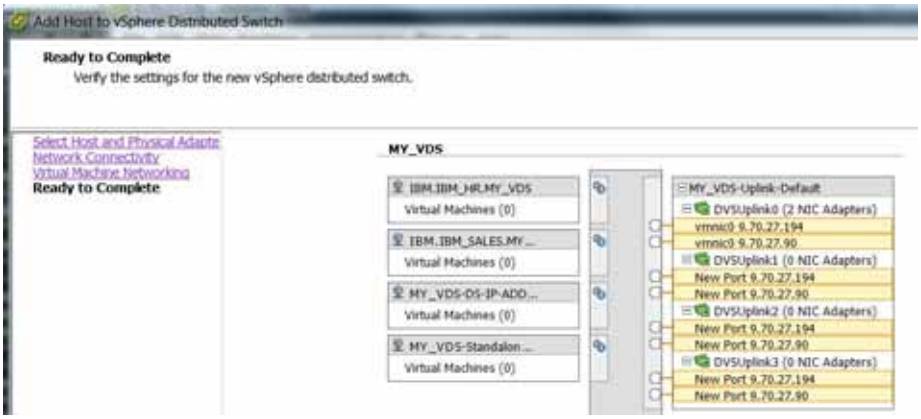
Attach ESXi Hosts to VDS

Before VMs on an ESXi host can communicate via the overlay network, the host needs to be attached to the VDS. From vCenter, go to **Home | Inventory | Networking** in the navigation bar, right click on the VDS, select “Add Host” from the menu and then select the hosts and physical adapters to add to the VDS:



Once desired hosts and physical adapters have been selected, click on “Next”:

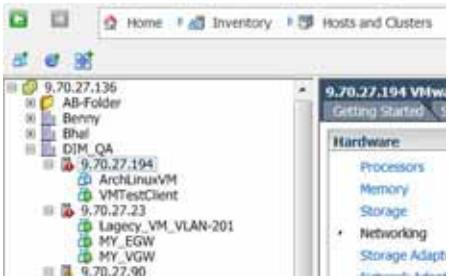
Then click on “Next”:



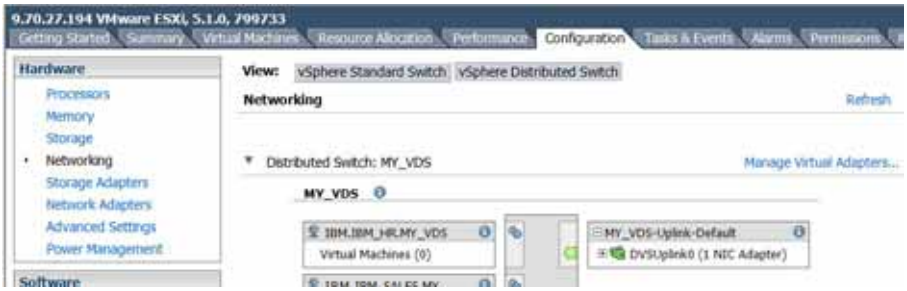
Finally, click on “Finish”:

Configure TEPs

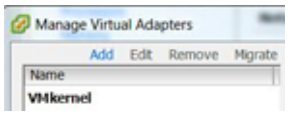
To configure the Tunnel End Point (TEP) on an ESXi host, first select **Inventory | Hosts and Clusters** in the navigation bar on vCenter, then select the host in question:



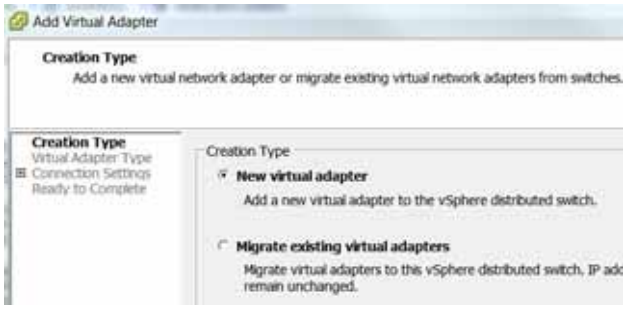
Go to the Configuration tab and select “Managed Virtual Adapters”:



In the “Manage Virtual Adapters” window, click Add:

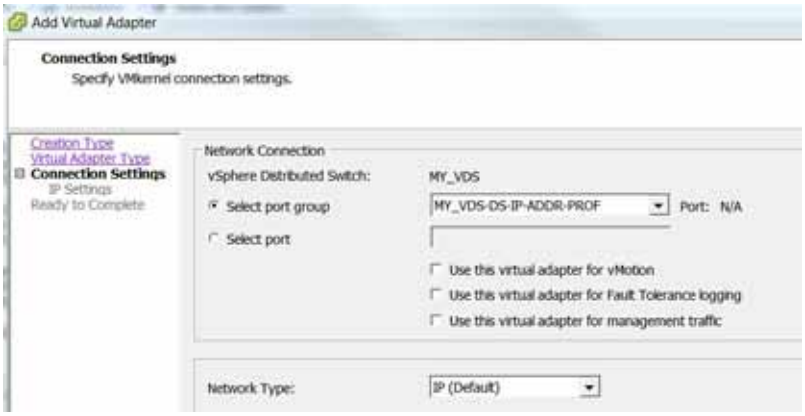


Select “New Virtual Adapter”:



Ensure that “VMkernel” is selected and click “Next”:

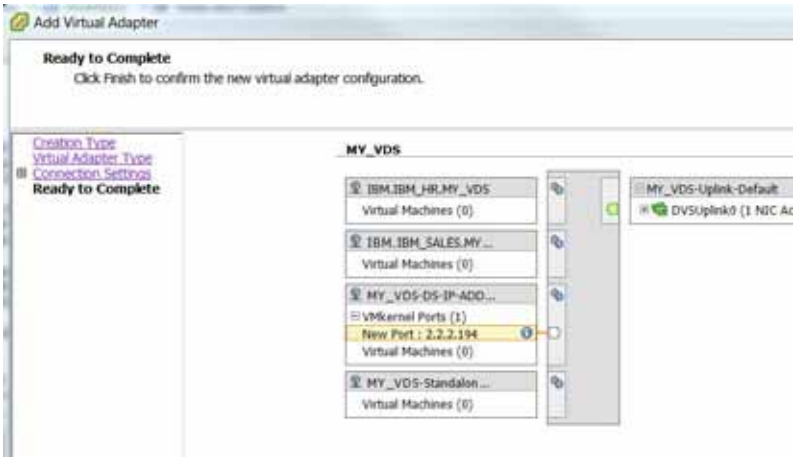
Then select the TEP Profile name for the Dove Tunnel as the port group and click “Next”:



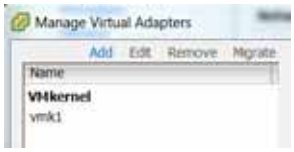
Note: Because this virtual adapter must be dedicated for TEP operation, it is required that the boxes for vMotion, Fault Tolerance logging, and management traffic must be left unchecked.

Enter the tunnel address and subnet mask and click “Next”:

Verify all the information and click Finish:



Verify that a new vmkernel adapter has been created:



Then close and at the DMC, verify that the TEP is registered via the “show switch-info” command:

```
DMC(config)# show switch-info
Dove-Tunnel-Endpoint-IP
=======================
2.2.2.194
```

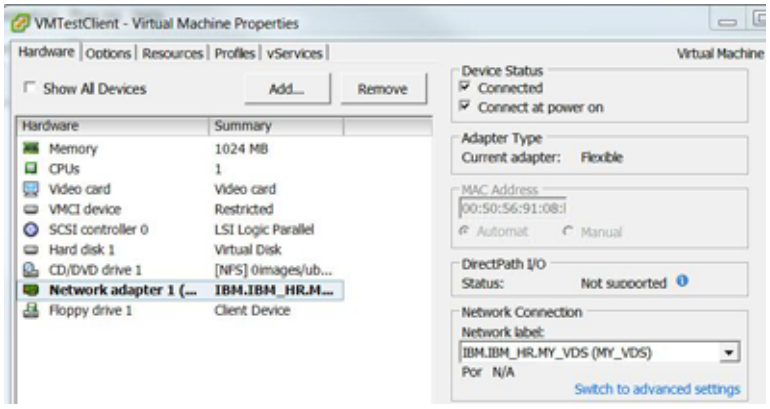
Repeat to register remaining ESXi hosts:

```
DMC(config)# show switch-info
Dove-Tunnel-Endpoint-IP
=======================
2.2.2.194
2.2.2.90
```

Attach End Systems

Note: This section assumes that end system VMs have already been deployed.

In vCenter, right click on the VM end system and select “Properties”. Change the network adapter to connect to the VDS and click “OK”:



Verify that the end system is attached in the DMC via the command:

show endpoints network [id] *<vnid>*

```
DMC(config)# show endpoints network id 1
 INDEX        HOST IP              VM MAC          VM IP        TUNNEL IP
=============================================================================
     1    9.70.27.194   00:50:56:91:08:b2      3.3.3.194        2.2.2.194
DMC(config)# show endpoints network id 2
 INDEX        HOST IP              VM MAC          VM IP        TUNNEL IP
=============================================================================
     1     9.70.27.90   00:50:56:91:08:b2       4.4.4.90         2.2.2.90
```

Part 2: Command Reference

Chapter 6. Command Basics

The IBM SDN VE system is ready to perform basic networking functions after initial installation. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

The SDN VE system provides an Command-Line Interface (CLI). Using a basic terminal, the CLI allows you to view information and statistics about the virtual network, and to perform any necessary configuration.

The CLI is available on any installed DOVE Management Console (DMC) where primary information and configuration is performed. A more limited CLI is also available on any installed DOVE Service Appliance (DSA), and is used mainly for initial setup purposes.

This chapter explains how to use the CLI available in the DOVE Management Console (DMC) and DOVE Service Appliance modules.

Login

CLI access is controlled through the use of a login name and password. Once you are connected to the system via SSH, you are prompted to enter a login name and password.

Default user name: `admin`

Default password: `admin`

Note: It is recommended that you change all default system password after initial configuration and as regularly as required under your network security policies.

Command Modes

Once logged in to the DMC or DSA, the CLI commands are organized by context. The various contexts, or *modes,* are organized in hierarchical fashion. The modes, their identifying prompts, and their navigational commands are shown in the following figure:

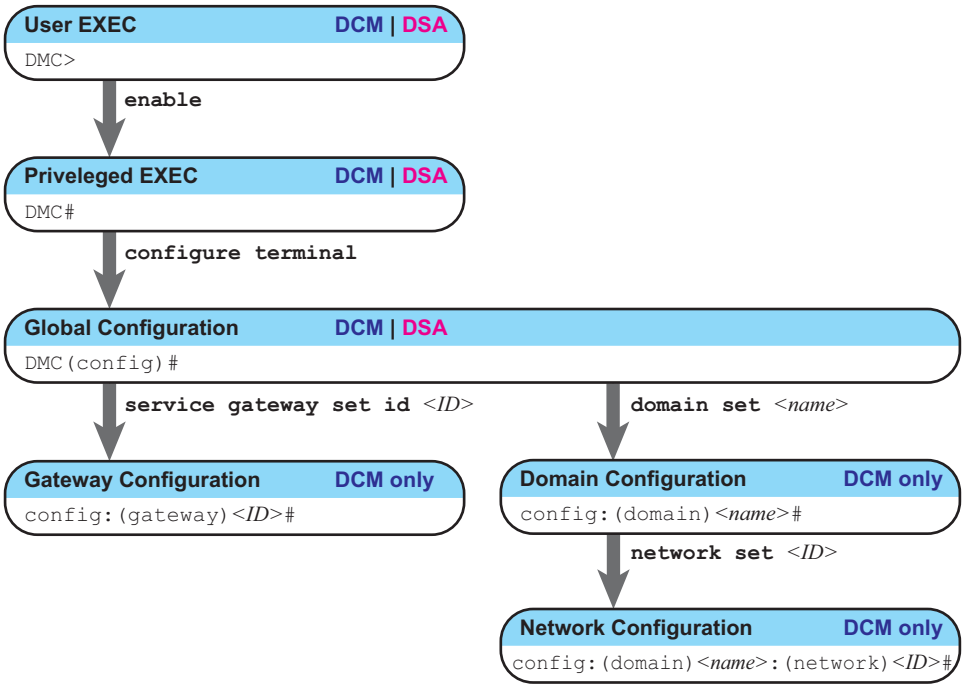


Figure 3. CLI Command Modes

User EXEC Mode

This is the initial access mode granted upon login. Only a limited set of commands is available in User EXEC mode. This mode is available in DMC and DSA nodes.

Identifying prompt:

```
DOVE>
```

Mode navigation commands:

- `enable`

  Enter Privileged EXEC mode.
- `exit` or `quit`

  Quit the CLI session.

Privileged EXEC Mode

This mode is used to collect information and execute limited operational commands. To avoid accidental configuration changes, commands that affect the permanent configuration are not permitted in this mode. Privileged EXEC mode is available in DMC and DSA nodes.

Use the following User EXEC mode command to access the Privileged EXEC mode:

```
DOVE> enable
```

Identifying prompt:

```
DOVE#
```

Mode navigation commands:

- `configure terminal`

  Enter Global Configuration mode.
- `exit`

  Return to User EXEC mode.
- `quit`

  Quit the CLI session.

Global Configuration Mode

This mode allows you to make changes to the running configuration. All changes take effect immediately (unless otherwise noted) and survive a reset of the system. This mode is available in DMC and DSA nodes.

Use the following Privileged EXEC mode command to access the Global Configuration mode:

```
DOVE# configure terminal
```

Identifying prompt:

```
DOVE(config)#
```

Several sub-modes are available from the Global Configuration mode. Each mode provides a specific set of commands.

Mode navigation commands:

- `service gateway set id <`*gateway ID*`>`

  Enter the Gateway Configuration mode. This mode is used for connecting virtual networks to traditional (non-virtual) networks.
- `domain set <`*domain name*`>`

  Enter the Domain Configuration mode. SDN VE domains and networks are configured in this mode.
- `exit`

  Return to Privileged EXEC mode.
- `quit`

  Quit the CLI session.

Gateway Configuration Mode

This mode is available in DMC modules only. Use this mode to define registered DOVE Gateway (DGWs) modules associated with the DMC. Gateways connect the SDN VE virtual network with traditional (non-virtual) networks.

Use the following Global Configuration mode command to access the Gateway Configuration mode:

```
DOVE(config)# service gateway set id <gateway ID>
```

where <*ID*> identifies the gateway you wish to configure. All related commands executed in the Gateway Configuration mode will be applied to the specified gateway.

Identifying prompt:

```
config:(gateway)<ID>#
```

Mode navigation commands:

- `exit`

  Return to Global Configuration mode.
- `quit`

  Quit the CLI session.

Domain Configuration Mode

This mode is available in DMC nodes only. Use this mode to define specific domains in the SDN VE system.

Use the following Global Configuration mode command to access the Domain Configuration mode:

```
DOVE(config)# domain set <name>
```

where <*name*> identifies the domain you wish to configure. All related commands executed in the Domain Configuration mode will be applied to the named domain.

Identifying prompt:

```
config:(domain)<name>#
```

Mode navigation commands:

- `network set id <network ID>`

  Enter the Network Configuration mode.
- `exit`

  Return to Global Configuration mode.
- `quit`

  Quit the CLI session.

Network Configuration Sub-Mode

This mode is available in DMC nodes only. This is a sub-mode of the Domain Configuration mode. Use this mode to define specific networks within a parent domain.

Access the Network Configuration mode via the Domain Configuration mode using the following command:

```
config:(domain)<name># network set id <network ID>
```

Where <*ID*> identifies the network you wish to configure. All related commands executed in the Network Configuration mode will be applied to the specified network within the parent domain.

Identifying prompt:

```
config:(domain)<name>:(network)<ID>#
```

Mode navigation commands:

- `exit`

  Return to Domain Configuration mode of the parent domain.
- `quit`

  Quit the CLI session.

Global Commands

Some basic commands are recognized throughout all CLI command modes. These commands are useful for obtaining online help and navigating through the interface.

Table 2. Description of Global Commands

Command	Action
`?`	List the commands available in the current mode, or when placed after a command keyword, provide further information about command options.
`exit`	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.

`find keyword`	Display the syntax for a specific command:
	`find keyword <keyword>`
	Or display the syntax of all current mode commands:
	`find`

`help`	List the commands available in the current mode.
`ping`	Use this command to verify station-to-station connectivity across the network. The format is as follows: `ping dst <destination IPv4 address> [src <source IPv4 address>]`
`quit`	Exit from the CLI and log out.

CLI Shortcuts

The following shortcuts allow you to enter commands more quickly and easily.

Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same mode. For example, consider the following full command and a valid abbreviation:

```
DOVE# configure terminal
```

or

```
DOVE# c t
```

Descriptor Omission

For commands that require you to specify parameters, the parameter descriptor portion (marked in blue throughout the following CLI chapters) is optional and may be omitted.

For example, the following command can be typed with descriptors for additional clarity, or without the descriptors for faster entry:

```
DMC(config)# clear switch-stats network-id 1 host-ip 9.70.27.194 mac
00:50:56:91:21:c9
```

```
DMC(config)# clear switch-stats 1 9.70.27.194 00:50:56:91:21:c9
```

Idle Timeout

By default, the CLI session will be disconnected after five minutes of inactivity. This function is controlled by the following command, which can be set from 1 to 60 minutes:

```
DMC(config)# system cli timeout mins <1-60>
```

Command mode:

Global Configuration mode

Chapter 7. DMC Show Commands

Once you have logged in to a DOVE Management Controller (DMC), you can view system configuration and statistical information using a variety of CLI `show` commands. The `show` commands are restricted from the User EXEC mode, but most are available globally in all other command modes.

In addition to commands that display small sets of specific information, there is also a command that displays all available information from all show commands in one list (known as an information dump):

```
show config
```

Please note that the output may exceed 10K of data, depending on your configuration.

If you want to capture the data to a file, such as for support or diagnostic purposes, set the communication software on your workstation to capture session data prior to issuing the command.

The remainder of this chapter discusses how to use each of the information-specific CLI `show` commands.

show cli-timeout

Show CLI Timeout

Any CLI session will be automatically logged out if idle for the length of time shown.

Syntax:

```
show cli-timeout
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show cli-timeout
CLI TIMEOUT 5 min
```

See also:

```
system cli timeout
```

`show config`

Show DMC Configuration

Show the current DMC configuration properties. This command consolidates the following information from various other show commands:

- Certificate Authority configuration
- DMC Version
- IPv4 Management Configuration
- Service Appliance Configuration
- Domain Configuration
- Network Configuration
- Policy Configuration
- Subnet Configuration
- Gateway Configuration
- High-Availability Configuration
- Underlay Network Configuration
- System Log Configuration

Please note that the output may exceed 10K of data, depending on your configuration.

If you want to capture the data to a file, such as for support or diagnostic purposes, set the communication software on your workstation to capture session data prior to issuing the command.

Syntax:

```
show config
```

Command mode:

Privileged EXEC and above

See also:

```
show tech-dump
```

show db-upgrade

Show Database Upgrade Status

Shows whether or not a database upgrade is required.

Syntax:

```
show db-upgrade
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show db-upgrade
DMC DB UPGRADE REQUIRED: No
```

See also:

```
system db-upgrade
```

show dcs-stats
Show Connectivity Services Statistics

Show DCS statistics for a given DCS node in a domain.

The display shows the total count and rate for the following events:

- Endpoint updates
- Endpoint lookups
- Policy lookups

Endpoints are MAC addresses of network adapters connected to the overlay network. The combination of network ID and MAC address uniquely identifies network adapters in the SDN VEsystem.

The counter values represent total counts. The rates are expressed as the number of receiving events per second.

Syntax:

`show dcs-stats node-id` *<node ID>* `domain-id` *<domain ID>*

Parameters:

<node ID>	DCS node ID as shown in `show service-appliance`.
<domain ID>	Domain ID (1-16777215) as shown in `show domain`.

Command mode:

Privileged EXEC and above

Example:

```
DMC# show dcs-stats node-id 1 domain-id 1
statistics for NODE 1 DOMAIN 1
-----------------------------------------------------------------
                                Counters             Rates
Endpoint update:                       0                 0
Endpoint lookup:                       0                 0
Policy lookup:                         0                 0
```

See also:

`show dcslist`

`show service-appliance`

`show domain`

show dcslist
Show DCS Domain List

Show DCS node IPv4 address for a specific domain, or for all domains.

Note: When the domain replication factor has changed (see "Update Domain Replication Factor" on page 176), the output of this command may temporarily show inconsistencies as the cluster configuration converges. These inconsistencies are normal and will not affect network processing. The display will resolve when the replication process is complete.

Syntax:

```
show dcslist domain <domain name>
```

Parameters:

<domain name> Target domain name (length 1-32 characters).

Command mode:

Privileged EXEC and above

Example

```
DMC# show dcslist domain denver
         DOMAIN_NAME                        DCS NODE IP
=============================================================
              DENVER                        9.70.27.151
```

See also:

```
service set-dcs-role
show service-appliance
```

show dmc-version

Show DMC Version

Show DOVE Management Console (DMC) software version information.

Syntax:

```
show dmc-version
```

Command mode:

Privileged EXEC and above

Example

```
DMC# show dmc-version
Version: 1.0.0 Mon Apr  8 12:12:23 PDT 2013
```

show dns

Show DMC DNS Addresses

Shows DMC domain nameserver addresses.

Syntax:

```
show dns
```

Command mode:

Privileged EXEC and above

Example

```
DMC# show dns
Index   IP
============================
    1   9.0.130.50
    2   9.0.128.50
```

Note: The DNS array indices will change if a member is deleted.

See also:

```
system dns add ip
system dns add cidr
system dns delete
```

show domain
Show Domains

Show information for all domains.

Syntax:

```
show domain
```

Command mode:

Privileged EXEC and above

Example

```
DMC# show domain
                                    Active/Total
Domain_ID       Domain_Name           Networks    Status
============================================================
        1            denver            3/      3  Active
        2            madrid            0/      0  Active
```

See also:

```
domain add
domain delete
```

show endpoints network

Show Endpoints

Show all endpoints on a given network.

Note: Endpoints that have multiple IPv4 addresses (as with IPv4 aliasing), there will be multiple entries for the endpoint's MAC address displayed.

Syntax:

```
show endpoints network id <ID>
```

Parameters:

<*ID*>	Network ID (1-16777215)

Command mode:

Privileged EXEC and above

Example:

```
DMC# show endpoints network id 1
       HOST IP             VM MAC                VM IP        TUNNEL IP
      ================================================================
      9.70.5.62  00:50:56:88:14:e8           1.1.1.100      20.0.0.101
```

See also:

```
show switch-info
show switch-stats
```

show export-list

Show Exported Profile List

Show a list of network configurations successfully exported to remote entities (such as DS 5000V switches).

Syntax:

```
show export-list [Remote-IP <remote IPv4>]
```

Parameters

<remote IPv4>	Optional. IPv4 address of the remote target entity. If omitted, exported networks for all remote entities will be listed.

Command mode:

Privileged EXEC and above

Example:

```
DMC(config)# show export-list Remote-IP 9.70.27.163
================================
Remote-IP            Network_ID
================================
9.70.27.163          10
```

See also:

export

unexport

show ext-mcast-networks

Show External Multicast Networks

Show external multicast network list.

This command displays designated network IDs used for handling external multicast traffic in the domain. If a network needs to send or receive external multicast traffic, appropriate policies need to be configured using ext-mcast-network IDs.

Syntax:

```
show ext-mcast-networks
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show ext-mcast-networks
Network_ID                    Network_Name    Domain_Name   Status
=====================================================================
  16777214               EXTMCAST_16777214           corp   Active
  16777213               EXTMCAST_16777213        sanjose   Active
  16777212               EXTMCAST_16777212         denver   Active
  16777211               EXTMCAST_16777211        finance   Active
  16777210               EXTMCAST_16777210         madrid   Active
```

show external-gateway fwd-rule

Show External Gateway Forward Rules

Show external gateway forward rules.

Syntax:

```
show external-gateway fwd-rule
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show external-gateway fwd-rule
 ID     PROTO   IP              PORT        REALIP           REALPORT    NETWORK_ID
=============================================================================================
 1      6       7.7.7.62        8080        1.1.1.52         80          6
 2      6       7.7.7.72        8080        1.1.1.52         80          7
 5      6       7.7.7.92        8080        1.1.1.52         80          9
 6      6       7.7.7.102       8080        1.1.1.52         80          10
 7      6       7.7.7.13        8080        1.1.1.52         80          11
 8      6       7.7.7.14        8080        1.1.1.52         80          11
```

See also:

```
external-gateway fwd-add-rule
external-gateway fwd-del-rule
```

show external-gateway list

Show external gateway configurations.

Syntax:

```
show external-gateway list
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show external-gateway list
NETWORK_ID: 1002                DOMAIN: D1
ID     IP               MIN_IP           MAX_IP           PORT-Range
=============================================================================
17     192.168.100.127  30.30.30.151     30.30.30.160     8000-8100
```

show external-gateway sessions

Show External Gateway NAT Sessions

Show information for specific external gateway Network Address Translation (NAT) sessions.

Syntax:

```
show external-gateway sessions gwindex <Gateway ID> type
<outbound|svcfwd|dynamic>
```

Parameters:

<Gateway ID>	External gateway ID.
type	The type parameter permits the following options: • outbound Display sessions from overlay network to external network. • svcfwd Display sessions from external network to overlay network via forwarding rules. • dynamic Display sessions created to handle one-to-one IPv4 mapping of external networks to overlay addresses.

Command mode:

Privileged EXEC and above

Example:

```
DMC# show external-gateway sessions gwindex 1 type outbound
DMC# show external-gateway sessions gwindex 1 type svcfwd
DMC# show external-gateway sessions gwindex 1 type dynamic
```

show gateway info

Show Gateway IPv4 Interface Configuration

Show gateway information.

Syntax:

```
show gateway info gwindex <Gateway ID> type <stats|ipv4|vnid-stats>
```

Parameters:

<Gateway ID>	External gateway ID.
`stats`	Display gateway statistics.
`ipv4`	Display gateway IPv4 interface configuration.
`vnid-stats`	Display gateway virtual network statistics.

Command mode:

Privileged EXEC and above

Example:

```
DMC# show gateway info gwindex 1 type ipv4
DMC# show gateway info gwindex 1 type stats
DMC# show gateway info gwindex 1 type vnid-stats
```

`show ha`

Show High-Availability Information

Shows a summary of high-availability (HA) information.

Syntax:

`show ha`

Command mode:

Privileged EXEC and above

Example:

```
DMC# show ha
HA STATUS=======================================
CLUSTER PEER IP:                9.70.27.16
DB NODE TYPE:                   Primary
DB CONNECTION STATE:            Connected
CLUSTER EXTERNAL IP:            9.70.27.245
NODE OWNS EXTERNAL ADDR:        Yes
```

See also:

`system ha type set`

show ha-external

Show HA Cluster External Address

Shows HA DMC cluster external address.

Syntax:

```
show ha-external
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show ha-external
EXTERNAL ADDRESS             9.70.27.245
```

See also:

```
system ha external set ip
system ha external set cidr
system ha external delete
```

show ha-peer

Show HA Peer Address

Shows the HA DMC peer's address.

Syntax:

```
show ha-peer
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show ha-peer
   PEER ADDRESS         9.70.27.54
```

See also:

```
system ha peer set ip
system ha peer set cidr
system ha peer delete
```

show ha-synchronization

Show HA Synchronization Status

Shows the status of database synchronization between primary node and secondary node.

Syntax:

```
show ha-synchronization
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show ha-synchronization
HA SYNCHRONIZATION STATUS:      Synchronized
```

See also:

```
system ha synchronization start
```

show ha-type

Show HA Node Type

Shows the HA node type.

Syntax:

```
show ha-type
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show ha-type
 TYPE              Primary
```

See also:

```
system ha type set
```

show ipmgmt

Show IPv4 Management Information

Shows DMC IPv4 address and netmask information.

Syntax:

```
show ipmgmt
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show ipmgmt
Manage IP Info
================================================================
      Method:                                          Dynamic
          IP:                                      9.70.27.32
        MASK:                                  255.255.255.0
```

See also:

```
system ipmgmt set ip
system ipmgmt set cidr
system ipmgmt set dhcp
```

show network

Show Networks

Show all networks in all domains.

Syntax:

```
show network
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show network
Network_ID             Network_Name       Domain_Name    Status
=================================================================
         1               Corp_Sales              CORP    Active
         2                  Corp_HR              CORP    Active
         3                Corp_MKT               CORP    Active
         4               Tech_Sales           SANJOSE    Active
         5                  Tech_HR           SANJOSE    Active
         6                Tech_MKT            SANJOSE    Active
```

See also:

```
network add
network set
```

show nexthop

Show DMC Gateway Address

Shows DMC gateway address (next hop).

Syntax:

```
show nexthop
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show nexthop
DMC NEXTHOP IP:      9.70.27.254
```

See also:

```
system nexthop set ip
system nexthop set cidr
system nexthop delete
```

show policy
Show Policy

Show policy between networks.

Syntax:

```
show policy
```

Command mode:

Domain Configuration mode

Network Configuration mode

Note: Not available in the other modes.

Example:

```
config:(domain)denver# show policy
   SRC DVG          DST DVG       TRAFFIC TYPE ACTION  PROVISIONED
=========================================================================
         1                2            unicast  allow      Y
         2                1            unicast  allow      Y
         2                3            unicast  allow      Y
         3                2            unicast  allow      Y
```

See also:

```
policy add
```

show replication-factor

Show Replication Factor of Domain

Show the currently configured replication factor for a specific domain. The replication factor represents the number of DCS nodes on which the system will attempt to copy the domain configuration. At least two nodes on different hosts are required for HA resilience.

Syntax:

```
show replication-factor domain <domain name>
```

Parameters:

<domain name> Target domain name (length 1-32 characters).

Command node:

Privileged EXEC and above

Example:

```
DMC# show replication-factor domain corp
DOMAIN_NAME : corp
Replication Factor : 2
```

See also:

```
update replication_factor
```

show service-appliance

Show Service Appliances

Show all DOVE Service Appliances (DSAs). Each type of DSA (DCS and DGW) are shown in separate tables. If a DCS has a role assigned, it is marked as `Y` in the information table. Otherwise as `N`.

Syntax:

```
show service-appliance
```

Command node:

Privileged EXEC and above

Example:

```
DMC# show service-appliance

DCS Service Appliances:
   ID         IP      SERVICE     ROLE      AGE_TIME   CONFIG      BUILT
                     CAPABILITY   ASSIGNED             VERSION   VERSION
  ================================================================================
    1    9.121.62.71        CS        Y        13 s   86/  86   1.0.0.130530
    2    9.121.62.72        CS        Y        15 s   86/  86   1.0.0.130530
    3    9.121.62.73        CS        Y        11 s   86/  86   1.0.0.130530
    4    9.121.62.74        CS        Y        12 s   86/  86   1.0.0.130530
    5    9.121.62.80        CS        N         7 s    0/  86   1.0.0.130530
    6    9.121.62.81        CS        N         3 s    0/  86   1.0.0.130530
    7    9.121.62.82        CS        N         3 s    0/  86   1.0.0.130530
    8    9.121.62.83        CS        N         7 s    0/  86   1.0.0.130530
    9    9.121.62.84        CS        N        13 s    0/  86   1.0.0.130530

GW Service Appliances:
   ID         IP      SERVICE     ROLE      AGE_TIME   CONFIG      BUILT
                     CAPABILITY   ASSIGNED             VERSION   VERSION
  ================================================================
    1    9.121.62.71        GW        N         7 s    0/  86   1.0.0.130530
    2    9.121.62.72        GW        N        15 s    0/  86   1.0.0.130530
    3    9.121.62.73        GW        N         0 s    0/  86   1.0.0.130530
    4    9.121.62.74        GW        N        15 s    0/  86   1.0.0.130530
    5    9.121.62.80        GW        Y         9 s   86/  86   1.0.0.130530
    6    9.121.62.81        GW        Y         8 s   86/  86   1.0.0.130530
    7    9.121.62.82        GW        Y         4 s   86/  86   1.0.0.130530
    8    9.121.62.83        GW        Y        11 s   86/  86   1.0.0.130530
    9    9.121.62.84        GW        Y         2 s   86/  86   1.0.0.130530
```

See also:

`set-dcs-role`

show subnet
Show Subnets

Show all subnets in the current Domain or Network Configuration mode.

Syntax:

```
show subnet
```

Command mode:

Domain Configuration mode

Network Configuration mode

Note: Not available in the other modes.

Example:

```
config:(domain)denver# show subnet
   ID        SUBNET(TYPE)           MASK        NEXTHOP       NETWORKS
================================================================================
    1      192.168.1.0(D)  255.255.255.0    192.168.1.1             1
                                                                    2
                                                                    3
    2      192.168.2.0(D)  255.255.255.0    192.168.2.1             1
                                                                    2
    3      192.168.3.0(D)  255.255.255.0    192.168.3.1             1

   (S)  ====>  Shared Subnet
   (D)  ====>  Dedicated Subnet
```

```
config:(domain)denver:(network)1# show subnet

   ID        SUBNET(TYPE)           MASK        NEXTHOP        NETWORK
================================================================================
    1      192.168.1.0(D)  255.255.255.0    192.168.1.1             1
    2      192.168.2.0(D)  255.255.255.0    192.168.2.1             1
    3      192.168.3.0(D)  255.255.255.0    192.168.3.1             1

   (S)  ====>  Shared Subnet
   (D)  ====>  Dedicated Subnet
```

See also:

```
show subnet domain
show subnet network
```

show subnet domain

Show Domain Subnets

Show all subnets in a named domain.

Syntax:

```
show subnet domain name <name>
```

Parameters:

<name>	Name of the target domain (1-32 characters).

Command mode:

Privileged EXEC and above

Example:

```
DMC# show subnet domain name denver

   ID        SUBNET(TYPE)           MASK         NEXTHOP       NETWORKS
=============================================================================
    1      192.168.1.0(D)  255.255.255.0    192.168.1.1             1
                                                                    2
                                                                    3
    2      192.168.2.0(D)  255.255.255.0    192.168.2.1             1
                                                                    2
    3      192.168.3.0(D)  255.255.255.0    192.168.3.1             1

   (S)  ====>  Shared Subnet
   (D)  ====>  Dedicated Subnet
```

See also:

```
show subnet
subnet network
```

show subnet network
Show Network Subnets

Show all subnets in a specific network.

Syntax:

```
show subnet network id <ID>
```

Parameters:

<*ID*>	Network ID (1-16713214) as shown in show network.

Command mode:

Domain Configuration mode

Example:

```
config:(domain)denver# show subnet network id 1

   ID        SUBNET(TYPE)           MASK         NEXTHOP         NETWORK
=============================================================================
    1      192.168.1.0(D)  255.255.255.0    192.168.1.1              1
    2      192.168.2.0(D)  255.255.255.0    192.168.2.1              1
    3      192.168.3.0(D)  255.255.255.0    192.168.3.1              1

   (S)  ====>  Shared Subnet
   (D)  ====>  Dedicated Subnet
```

See also:

```
show subnet
show subnet domain
```

show switch-info

Show Switch Information

Show information for DS 5000V switches that have registered with the DMC.

Syntax:

```
show switch-info
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show switch-info
Dove-Tunnel-Endpoint-IP
=======================
10.50.116.101
10.50.116.100
10.50.116.106
10.50.116.105
```

See also:

```
show switch-stats
show endpoints
```

show switch-stats
Show Switch Statistics

Show end point port statistics for a given network ID, switch host IPv4 address and optional MAC address. If the MAC address is included, the statistics for that particular end-point will be displayed. If the MAC address is omitted, the aggregated statistics for all the end-points on the specified network ID and switch IPv4 address will be displayed.

Syntax:

```
show switch-stats network-id <ID> <host IPv4 address> [<MAC address>]
```

Parameters:

<ID>	Target virtual network ID (1-16777215).
<host IPv4 address>	Target switch management IPv4 address.
<MAC address>	Optional MAC address of the target end-point.

Command mode:

Privileged EXEC and above

Example:

```
DMC# show switch-stats network-id 99 10.20.30.40
======================================================================
Statistics for vnid 99
                                In counters           Out counters
----------------------------------------------------------------------
Bytes                                3879482               99489485
UcastPkts                                200                   1100
BroadcastPkts                            300                   1200
MulticastPkts                              0                     40
DiscardPkts                                5                      3
ErrorPkts                                  6                      1

Ingress Discard reasons for vnid 99
UnknownProtosPkts                         70
VlanDiscards                              80
ACLDiscards                               90
EmptyEgress                               10
```

See also:

```
clear switch-stats
show endpoints
show network
```

show syslog

Show System Log Configuration

Show DMC system log configuration status for each module.

Syntax:

```
show syslog
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show syslog
   Syslog settings
   ================================================
   module-name     log-level       state
   ------------------------------------------------
   dove-cli        emergency       disable
   dps-api         emergency       disable
   dgw-api         emergency       disable
   dsw-api         debug           disable
   sys-api         emergency       enable
   vrmgr-api       emergency       disable
   raw-proto       emergency       disable
```

See also:

```
syslog set
syslog log-level
```

show system acknowledgement

Show System Acknowledgement & Licensing Information)

Show software licensing information for elements used in the SDN VE system.

Syntax:

```
show system acknowledgement
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show system acknowledgement
```

`show tech-dump`

Show Tech Dump File

Show system technical information. This command consolidates the following system, configuration, and run time information from various other show commands:

- Certificate Authority configuration
- DMC Version
- IPv4 Management Configuration
- Service Appliance Configuration
- Domain Configuration
- Network Configuration
- Policy Configuration
- Subnet Configuration
- Gateway Configuration
- High-Availability Configuration
- Underlay Network Configuration
- System Log Configuration
- Switch Information

Please note that the output may exceed 10K of data, depending on your configuration.

If you want to capture the data to a file, such as for support or diagnostic purposes, set the communication software on your workstation to capture session data prior to issuing the command.

Syntax:

```
show tech-dump
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show tech-dump
```

See also:

`show config`

show terminal-length
Show Terminal Length

Show the number of lines displayed per screen. To facilitate reading lengthy output, the display for commands that produce more lines than defined by the terminal length will automatically pause, requiring a keypress before resuming each page of output.

Syntax:

`show terminal-length`

Command mode:

Privileged EXEC and above

Example:

```
DMC# show terminal-length
38 lines per screen
```

See also:

`terminal-length`

show underlay-network

Show Underlying Physical Network

Shows the configured physical networks that TEPs connect to.

Syntax:

```
show underlay-network
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show underlay-network
   ID            NET           MASK        NEXTHOP
=========================================================
    1        1.1.1.0  255.255.255.0        1.1.1.1
    2        2.2.2.0  255.255.255.0        2.2.2.1
```

See also:

```
underlay-network add
underlay-network del
```

`show vlan-gateway`

Show VLAN Gateway Configuration

Show VLAN gateway configuration.

Syntax:

```
show vlan-gateway
```

Command mode:

Privileged EXEC and above

Example

```
DMC# show vlan-gateway
   ID                  IP   VLAN_ID NETWORK_ID DOMAIN_ID
=============================================================
    1         9.70.27.177       201          1         1
```

See also:

`vlan-gateway add`

Chapter 8. DMC Configuration Commands

This chapter discusses how to use the individual CLI for making configuration changes.

clear screen

Clear Screen

Clear the terminal screen.

Syntax:

```
clear screen
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# clear screen
```

clear switch-stats

Clear Switch Statistics

Clear DS 5000V end point port statistics for a given network ID, switch host IPv4 address, and optional MAC address. If the MAC address is supplied, the statistics for that particular end-point will be cleared. If MAC address is omitted, the aggregated statistics for all the end-points on the specified switch host IPv4 address under the given network ID will be cleared.

Syntax:

```
clear switch-stats network-id <network ID> host-ip <host IPv4 address>
[mac <MAC address>]
```

Parameters:

<network ID>	The target virtual network ID (1-16777215).
<host IPv4 address>	The target switch's management IPv4 address.
<MAC address>	Optional. The MAC address of a specific end-point.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# clear switch-stats network-id 1 host-ip 9.70.27.194 mac
00:50:56:91:21:c9
```

See also:

```
show switch-stats
show endpoints
show network
```

domain add

Domain Addition

Create and name a new domain, if it does not already exist.

Syntax:

`domain add name` <*domain name*>

Parameters:

<*domain name*> The name of the target domain (1-32 characters).

Command mode:

Global Configuration mode

Example:

```
DMC(config)# domain add name Denver
```

See also:

`show domain`
`domain delete`
`domain set`

domain delete
Domain Deletion

Delete an existing domain either by domain ID or name.

Syntax:

```
domain delete id <domain ID>
domain delete name <domain name>
```

Command mode:

Global Configuration mode

Parameters:

<domain ID>	The ID of the target domain as shown with the `show domain` command.
<domain name>	The name of the target domain.

Examples:

```
DMC(config)# domain delete id 1
DMC(config)# domain delete name corp
```

See also:

```
show domain
domain add
domain set
```

domain set
Domain Configuration Mode

Enter the Domain Configuration mode, where parameters for the named domain can be set, including access to the Network Configuration sub-mode. To exit the Domain Configuration mode, use the `exit` command.

Syntax:

`domain set name` <*domain name*>

Command mode:

Global Configuration mode

Parameters:

<*domain name*>	Name of the target domain context (1-32 characters). To prevent confusion with domain indices, the name cannot begin with a numeric character.

Example:

```
DMC> enable
DMC# configure terminal
DMC(config)# domain set name Denver
config:(domain)Denver#
```

See also:

`domain add`
`domain delete`
`show domain`

`exit`

Exit the Current Context Mode

Exit from a context sub-mode and return to the parent mode. If already at the top level, exit from the command line interface and log out.

Syntax:

`exit`

Command mode:

All

Example:

```
config:(domain)corp:(network)1# exit
config:(domain)corp# exit
DMC(config)# exit
DMC# exit
DMC>
```

See also:

`quit`

`export`

Export a Network Profile

Export the specified network configuration to a remote entity.

If the remote entity is a DS 5000V, a profile named `domain.network.vds-name` will be created on the vSwitch, and saved with a VNID set to the specified network ID.

By default, exported profiles will be created on the DS 5000V with 10 ports. Use the CLI present on the DS 5000V to add or remove ports (`config-dvprof` mode `addports` or `delports`).

Syntax:

`export Network_ID` *<network ID>* `ip-addr` *<remote IPv4>*

Parameters:

<network ID>	Network ID (1-16713214) to export.
<remote IPv4>	IPv4 address of remote target entity.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# export Network_ID 10 ip-addr 9.70.27.163
```

See also:

`unexport`

`short export-list`

external-gateway add

External Gateway Addition

Associate external IPv4 addresses with the overlay network.

This command enables external connectivity for overlay entities connected to the given VNID. This command associates the specified IPv4 address or addresses with the given VNID. The IPv4 address(es) and range of ports are used to multiplex traffic (NAT) from different overlay VMs to the external network.

Syntax:

```
external-gateway add dgw-index <gateway> extip-range
<IPv4 start>[-<IPv4 end>] port-range <port start>-<port end>
```

Parameters:

<gateway>	Target gateway index (1-65535).
<IPv4 start>	First external IPv4 address in the target range.
<IPv4 end>	Optional. Last external IPv4 address in the target range.
<port start>	First port in the target range
<port end>	Last port in the target range

Command mode:

Network Configuration mode

Examples:

```
config:(domain)Denver:(network)1# external-gateway add dgw-index 1 extip-range
9.70.25.10 port-range 8000-9000
```

```
config:(domain)Denver:(network)1# external-gateway add dgw-index 1 extip-range
9.70.25.10-9.70.25.20 port-range 8000-9000
```

external-gateway fwd-add-rule

External Gateway Forwarding Rule Addition

Add a service port forwarding rule for an external gateway within the current domain and network context. This enables external networks to access a service hosted in the overlay network.

Syntax:

```
external-gateway fwd-add-rule dgw_index <gateway ID> extip
<external IPv4> protocol <protocol> port <logical port> overlayip
<overlay IPv4> overlayport <overlay port> [proxyip-range
<proxy start>-<proxy end>]
```

Parameters:

<gateway ID>	Gateway Index (1-65534).
<external IPv4>	External gateway IPv4 address.
<protocol>	Well-known protocol number (0-254). For example:

Number	Name
0	Any (match any protocol)
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF
112	VRRP

<logical port>	Logical port number. This value is protocol dependent: 1-65534 for protocols 6 (TCP) and 17 (UDP) 0 for all other protocols.
<overlay IPv4>	IPv4 address for overlay service (VM).
<overlay port>	Overlay service port (0-65534). This value is protocol dependent: 1-65534 for protocols 6 (TCP) and 17 (UDP) 0 for all other protocols.
<proxy start>	Part of the optional `proxyip-range` parameter. Specifies the first IPv4 address in the proxy IPv4 address range.
<proxy end>	Part of the optional `proxyip-range` parameter. Specifies the last IPv4 address in the proxy IPv4 address range.

Command mode:

Network Configuration mode

Example:

```
config:(domain)Denver:(network)10# external-gateway fwd-add-rule dgw_index 9 extip
20.210.20.100 protocol 6 port 5001 overlayip 192.168.1.2 overlayport 5001
```

See also:

`show external-gateway fwd-rule`

`external-gateway fwd-del-rule`

`external-gateway fwd-del-rule`

External Gateway Forwarding Rule Deletion

Delete a service port forwarding rule from an external gateway within the current domain and network context.

Syntax:

`external-gateway fwd-del-rule dgw_index <gateway ID> extip <external IPv4> protocol <protocol> port <logical port>`

Parameters:

<gateway ID>	Gateway Index (1-65534).
<external IPv4>	External gateway IPv4 address.
<protocol>	Well-known protocol number (0-254). For example:

Number	Name
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF
112	VRRP

<logical port>	Logical port number. This value is protocol dependent: 1-65534 for protocols 6 (TCP) and 17 (UDP) 0 for all other protocols.

Command mode:

Network Configuration mode

Example:

```
config:(domain)corp:(network)1# external-gateway fwd-del-rule dgw_index 2 extip
20.38.1.21 protocol 6 port 22
```

See also:

`show external-gateway fwd-rule`

`external-gateway fwd-add-rule`

`find`

Find Command Syntax

Find commands and display command syntax.

Syntax:

`find [keyword <keyword>]`

Parameters:

<keyword>	Optional. If present, the syntax for any matching command will be displayed. If omitted, syntax for all commands in the current context mode will be displayed.

Command mode:

All

Example:

```
DMC(config)# find keyword unexport
Unexport a Network
        unexport <Network_ID (1-16713214)> <ip-addr>
```

ip-add
IPv4 Interface Addition

Use this command to add either a SDN VE tunnel endpoint IPv4 address or an external gateway IPv4 address for the current Dove Gateway (DGW) appliance context.

Syntax:

```
ip-add ip addr <base IPv4 address> mask <IPv4 mask> nexthop <gateway IPv4> type {dovetunnel|external} [vlan <VLAN ID>]
```

Parameters:

<*base IPv4 address*> Base IPv4 address of the IPv4 interface

<*range mask*> IPv4 address mask used with the base IPv4 address to create an IPv4 address range for the interface.

<*gateway IPv4*> The gateway (next hop) for this interface.

`type` The type parameter permits the following options:

- `dovetunnel`

  Add an SDN VE tunnel endpoint IPv4 address. The interface defines an IPv4 address to communicate with SDN VE switches and other SDN VE gateways. This IPv4 address will be used in SDN VE encapsulation headers.

- `external`

  Add an external network IPv4 address for external gateway operation. The interface is used to communicate with external networks without SDN VE encapsulation headers.

<*VLAN ID*> Optional. Specify the VLAN ID (1-4094) of this interface.

Command mode:

Gateway Configuration mode

Examples:

```
config:(gateway)1# ip-add ip addr 1.1.1.10 mask 255.255.255.0 nexthop 1.1.1.254 type dovetunnel
```

```
config:(gateway)1# ip-add ip addr 1.1.1.10 mask 255.255.255.0 nexthop 1.1.1.254 type dovetunnel vlan 100
```

```
config:(gateway)2# ip-add ip addr 9.70.25.5 mask 255.255.255.0 nexthop 9.27.25.254 type external
```

```
config:(gateway)2# ip-add ip addr 9.70.25.5 mask 255.255.255.0 nexthop 9.27.25.254 type external vlan 200
```

See also:

`ip-del`

`ip-del`

IPv4 Interface Deletion

Delete an existing IPv4 interface from the current DOVE Gateway (DGW) appliance context.

Syntax:

`ip-del ip addr` *<IPv4 address>*

Parameters:

<IPv4 address> Target IPv4 interface address.

Command mode:

Gateway Configuration mode

Example:

```
config:(gateway)1# ip-del ip addr 9.70.25.5
```

See also:

`ip-add`

network add

Network Addition

Create a new network within the current domain context.

Network names and IDs must be unique within a domain, but may be reused in other domains.

Syntax:

```
network add id <network ID> name <name>
```

Parameters:

<network ID>	Target network ID (1-16713214).
<name>	Target network name.

Command mode:

Domain Configuration mode

Examples:

```
config:(domain)Denver# network add 1 Corp_Sales
config:(domain)Denver# network add 2 Corp_HR
config:(domain)Denver# network add 3 Corp_MKT
```

See also:

```
network delete
network set
show network
```

network delete
Network Deletion

Delete an existing network from the current domain context.

Syntax:

```
network delete id <network ID>
```

Parameters:

<network ID> The target network ID (1-16713214).

Command mode:

Domain Configuration mode

Example:

```
config:(domain)Denver# network delete id 3
```

See also:

```
network add
network set
show network
```

network set

Network Configuration Mode

Enter the Network Configuration mode. Network commands within the Network Configuration mode apply only to the specified network within the current domain context. From within this mode, networks can be bound to subnets and gateways.

Network IDs must be unique within a domain, but may be reused in other domains.

To exit the Network Configuration mode, use the `exit` command.

Syntax:

```
network set id <network ID>
```

Parameters:

<network ID> The target network ID within the current domain.

Command mode:

Domain Configuration mode

Example:

```
DMC> enable
DMC# configure terminal
DMC(config)# domain set name Denver
config:(domain)Denver# network set id 1
config:(domain)Denver:(network)1#
```

See also:

`network add`

`network delete`

`show network`

`ping`

Ping Test Network Connection

Use the ping utility to test network connectivity.

Syntax:

`ping dst` <*destination IPv4*> `[src` <*source IPv4*>`]`

Parameters:

<*destination IPv4*> Destination IPv4 address.

<*source IPv4*> Optional source IPv4 address.

Command mode:

All

Example:

```
DMC# ping dst 9.0.130.50
PING 9.0.130.50 (9.0.130.50): 56 data bytes
64 bytes from 9.0.130.50: seq=0 ttl=115 time=76.719 ms
64 bytes from 9.0.130.50: seq=1 ttl=115 time=76.528 ms
64 bytes from 9.0.130.50: seq=2 ttl=115 time=76.730 ms
64 bytes from 9.0.130.50: seq=3 ttl=115 time=78.763 ms
--- 9.0.130.50 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 76.528/77.185/78.763 ms
```

policy add

Policy Addition

Define a policy for traffic between two networks within the current domain context. Each policies can be applied to unicast or multicast traffic types, and defined to allow or drop matching packets.

Syntax:

```
policy add peers <network ID1>:<network ID2> traffic-type
{unicast|multicast} action {drop|allow}
```

Parameters:

<network ID1&2> Network peers

Command mode:

Domain Configuration mode

Example:

```
config:(domain)corp# policy add peers 1:2 traffic-type unicast action allow
```

See also:

`show policy`

quit

Quit the ICSLI Session

Exit from the CLI and log out.

Syntax

quit

Command mode:

All

Example:

```
config:(domain)corp:(network)1# quit
```

See also:

exit

`remove-subnet`

Remove a Subnet from a Network

Remove an existing subnet from the current domain and network context.

In order to fully remove a subnet from the SDN VE configuration, all DCS nodes (with DCS role shown as `Y` in the `show service-appliance` output) must be currently available on the network. If assigned DCS nodes are unavailable, the DMC will retain the target subnet information. The configuration elements pertaining to the deleted subnet will not be cleared from the DMC until the DCS nodes are made available on the network, or until their DCS roles have been reset using the `service reset-dcs-role` command.

Syntax:

`remove-subnet index` <*subnet index*>

Parameters:

<*subnet index*> Subnet index as shown in the `show subnet` command.

Command mode:

Network Configuration mode

Example:

```
config:(domain)corp:(network)3# remove-subnet index 1
```

See also:

`show subnet`
`show subnet domain`
`show subnet network`
`subnet index`

service delete-dcs
Delete a DCS Node

Remove a DOVE Connectivity Service (DCS) appliance from the system.

This command can be applied only to a DCS that has no current role assigned: either its underlying DSA has not yet been assigned, or the module has been reset to its basic DSA function, removing the DCS role. To reset the role of a currently assigned DCS prior to deletion, use the `service reset-dcs-role` command.

Syntax:

`service delete-dcs id <DCS ID>`

Parameters:

<DCS ID>	DCS appliance ID as shown with the `show service-appliance` command.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# service delete-dcs id 3
```

See also:

`show dcslist`
`service reset-dcs-role`
`service set-dcs-role`
`show service-appliance`

service delete-dgw
Delete a DGW Node

Remove a DOVE Gateway (DWG) service appliance node from the system.

This command can be applied only to a DGW that has no current role assigned: either its underlying DSA has not yet been assigned, or the module has been reset to its basic DSA function, removing the DGW role. To reset the role of a currently assigned DGW prior to deletion, use the `service reset-dgw-role` command.

Syntax:

```
service delete-dgw id <gateway ID>
```

Parameters:

<gateway ID>	DGW service appliance ID as shown with the `show service-appliance` command.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# service delete-dgw-role id 3
```

See also:

```
show service-appliance
service set-dgw-role
service reset-dgw-role
```

service gateway set

Gateway Configuration Mode

Enter the Gateway Configuration mode, where parameters for the named gateway can be set. To exit the Gateway Configuration mode, use the `exit` command.

Syntax:

```
service gateway set id <gateway ID>
```

Parameters:

<gateway ID>	The GW node ID (1-65534) as shown with the show service-appliance command.

Command mode:

Global Configuration mode

Example:

```
DMC> enable
DMC# configure terminal
DMC(config)# service gateway set id 1
config:(gateway)1#
```

See also:

`show service-appliance`

`ipv4-add`

service reset-dcs-role
Reset DCS Node Role

Reset the role of a DOVE Connectivity Service (DCS) node.

The role of a DCS can be reset only if it will not result in the loss of unique domain information. If the DCS is the only one in the cluster to serve certain domains, the role cannot be reset. The role may be reset only if the DCS is presently serving no domains, or if serving domains which are also held in common with other DCS modules in the cluster.

If the DCS role reset fails, check that the number of active and synchronized DCS nodes meets the minimum replication factor of two.

Syntax:

```
service reset-dcs-role id <DCS ID>
```

Parameters:

<DCS ID>	DCS node ID (1-65534) as shown in the `show service-appliance` command.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# service reset-dcs-role id 1
```

See also:

```
show dcslist
service set-dcs-role
show service-appliance
```

service reset-dgw-role
Reset DGW Node Role

Reset the role of a registered DOVE Gateway (DGW) service appliance node. This is permitted only when all the associated gateway configuration elements have been deleted from the domain.

Syntax:

```
service reset-dgw-role id <DGW ID>
```

Parameters:

<DGW ID>	GW node ID as shown with the `show service-appliance` command.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# service reset-dgw-role id 3
```

See also:

```
show service-appliance
service set-dgw-role
```

service set-dcs-role

Assign DCS Role to DSA

Assign a list of DOVE Service Appliances (DSAs) to act as DOVE Connectivity Service (DCS) nodes.

Each DSA can be assigned either a DCS or DGW role. These roles are mutually exclusive. The DCS role can be applied only to DSAs that have no current role assigned. If a target DSA is presently operating in a DGW role, the role must be reset prior to assigning the DCS role (see the `service reset-dgw-role` command).

Syntax:

```
service set-dcs-role ids <DSA list>
```

Parameters:

<DSA list>	A comma-separated list of target DSA node IDs. IDs are as shown in the `show service-appliance` command.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# service set-dcs-role ids 1,2
```

See also:

```
show dcslist
service reset-dcs-role
service reset-dgw-role
show service-appliance
```

service set-dgw-role

Assign Gateway Role to DSA

Assign a registered DOVE Service Appliance (DSAs) to act as a Dove Gateway (DGW) node. Setting this role will allow gateway related configuration on the DSA.

Each DSA can be assigned either a DGW or DCS role. These roles are mutually exclusive. The DGW role can be applied only to DSAs that have no current role assigned. If a target DSA is presently operating in a DCS role, the role must be reset prior to assigning the DGW role (see the `service reset-dcs-role` command).

Syntax:

```
service set-dgw-role id <DSA ID>
```

Parameters:

<DSA ID>	DSA ID of target gateway appliance. DSA IDs are shown in the `show service-appliance` command.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# service set-dgw-role id 3
```

See also:

```
show service-appliance
service reset-dgw-role
```

`show`

Show Information

You can view SDN VE configuration and statistical information using a variety of `show` commands. For details, see “DMC Show Commands” on page 77.

subnet add

Subnet Addition

Create a new subnet if it doesn't already exist. This will create a new entry in the DMC database that can be later associated with virtual networks (VNIDs).

Syntax:

```
subnet add net <base IPv4 address> mask <netmask> nexthop
<gateway IPv4> type {shared|dedicated}
```

Parameters:

<base IPv4 address>	Base IPv4 address of the IPv4 subnet
<netmask>	IPv4 address mask used with the IPv4 address to create an IPv4 subnet range.
<gateway IPv4>	The gateway (next hop) for this IPv4 subnet.
`type`	Two types of subnets are permitted: `shared` or `dedicated`. Each specific network can be associated with only one type at a time.

Command mode:

Domain Configuration mode

Example:

```
config:(domain)corp# subnet add net 1.1.0.0 mask 255.255.0.0 nexthop 1.1.1.1 type
dedicated
```

See also:

`show subnet`
`subnet delete`
`subnet index`

subnet delete
Subnet Deletion

Delete a previously configured subnet from the current domain context.

Syntax:

`subnet delete id <subnet ID>`

Parameters:

<subnet ID>	Subnet ID (1-16777215) as shown in the show subnet command.

Command mode:

Domain Configuration mode

Example:

```
config:(domain)corp# subnet delete id 1
```

See also:

`show subnet`

`subnet add`

subnet index

Bind a Subnet to a Network

This command will associate a configured subnet with the current virtual network. The command will send a REST message to the DCS modules and all VLAN gateways and external gateways that are part of the current domain and network context.

Syntax:

`subnet index <subnet index>`

Parameters:

<*subnet index*> Subnet index as shown in the `show subnet` command.

Command mode:

Network Configuration mode

Example:

```
config:(domain)corp:(network)2# subnet index 2
```

See also:

`show subnet`
`show subnet domain`
`show subnet network`
`remove-subnet`
`subnet add`

syslog console action

System Log Console Control

Enable or disable console logging for all modules (processes). When enabled, log messages are sent to the DMC console. Console logging is disabled by default.

Syntax:

```
syslog console action {enable|disable}
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# syslog console action enable
```

See also:

```
syslog set
syslog log-level
```

syslog log-level
System Log Levels

Set the log level for a specific module (process). Logging messages are stored in the `/flash/dmc_syslog.log` file. Use this command in conjunction with the `syslog set` command to control logging. Logging is disabled by default.

Syntax:

```
syslog log-level module-name <module> level <log level>
```

Parameters:

<module> The name of the target module:

- `raw-proto`
- `dsw-api`
- `dps-api`
- `vrmgr-api`
- `dgw-api`
- `dove-cli`
- `sys-api`

<log level> The log level of the target module:

- `debug`
- `warn`
- `info`

Command mode:

Global Configuration mode

Example:

```
DMC(config)# syslog log-level module-name dps-api level debug
```

See also:

`syslog set`
`syslog console`
`show syslog`

syslog set

System Log Module Control

You can enable or disable logging for specific modules (processes). Log messages are stored in the `/flash/dmc_syslog.log` file. Use this command in conjunction with the other `syslog` commands to control logging. Logging is disabled by default.

Syntax:

```
syslog set module-name <module> action {enable|disable}
```

Parameters:

<module> The name of the target module:

- `raw-proto`
- `dsw-api`
- `dps-api`
- `vrmgr-api`
- `dgw-api`
- `dove-cli`
- `sys-api`

Command mode:

Global Configuration mode

Example:

```
DMC(config)# syslog set module-name dps-api action enable
```

See also:

`syslog log-level`
`syslog console`
`show syslog`

system cli timeout

CLI Idle Timeout

Sets length of time before CLI times out.

Syntax:

```
system cli timeout mins <minutes>
```

Parameters:

<minutes>	Timeout period in minutes.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system cli timeout mins 8
```

See also:

```
show cli-timeout
```

system db-upgrade
Start Database Upgrade

Begin the database upgrade process.

This function will work in the background. Use the `show db-upgrade` command to check the status of the upgrade process.

Syntax:

`system db-upgrade`

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system db-upgrade
```

See also:

`show db-upgrade`

system dmc-corefiles action
DMC Core-Dump File Control

This command controls the DMC core-dump files which are generated when an unexpected system halt occurs. These files contain debugging information for field support.

The core dump files are located in the following directory:

`/flash/sdn/uld/httpd/techdump/tech-support/core`

The files use following file naming convention:

<process name>_<time-stamp> - <signal number> . <process ID>

where:

<process name> = The name of the process that caused the halt.

<time-stamp> = The number of seconds since Jan. 1, 1970.

<signal number> = The signal code generated at the time of the crash.

<process ID> = The process ID.

Syntax:

```
system dmc-corefiles action {enable|disable|clean|downloadable}
```

Parameters (`action`):

`enable`	Enable core dump files generation
`disable`	Disable core dump files generation
`clean`	Remove core dump files
`downloadable`	Enable core dump file download

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system dmc-corefiles action enable
Core dump file: dove_cli.py_1369270836-11.832
```

system dmc-upgrade

Upgrade DMC Software Image

Upgrade the DMC software image. The new image file must be accessible to the DMC. Once upgraded, the DMC will automatically reboot in order to run the new image. You can verify the upgrade by using the `show dmc-version` command.

Syntax:

`system dmc-upgrade url` *<image URL>*

Parameters:

<image URL> URL (1 to 128 characters) for the DMC software image file.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system dmc-upgrade url
ftp://9.111.86.13/xyl/ibm-sdn-dmc-upgrade-1.0.0.img
Please wait while the DMC Image is being upgraded!!
DMC(config)#
```

See also:

`show dmc-version`

`system reload`

system dns add
Nameserver Addition

Set the nameserver address by specifying an IPv4 address and network mask or CIDR designation.

Syntax:

```
system dns add ip ip <IPv4 address> mask <netmask>
system dns add cidr <CIDR>
```

Parameters:

<IPv4 address>	DNS IPv4 address in dotted decimal notation (a.b.c.d).
<netmask>	DNS IPv4 netmask in dotted decimal notation (a.b.c.d).
<CIDR>	DNS IPv4 address in CIDR format (a.b.c.d/e).

Command mode:

Global Configuration mode

Examples:

```
DMC(config)# system dns add ip ip 10.10.0.1 mask 255.255.255.0
DMC(config)# system dns add cidr 10.10.0.1/24
```

See also:

```
show dns
system dns delete
```

system dns delete

DNS Deletion

Clear a DMC nameserver address.

Syntax:

```
system dns delete index <DNS ID>
```

Parameters:

<DNS ID>	The index of the nameserver as shown in the `show dns` command. Note that DNS array indices will change as members are added or deleted.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system dns delete index 1
```

See also:

```
show dns
system dns add ip
system dns add cidr
```

system ha convert

Convert Standalone DMC to HA DMC

Start the process of converting a standalone DMC node to a high-availability (HA) DMC node by specifying a new node IPv4 address and mask or CIDR designation.

This replaces the standalone node address with the one specified in the command, and uses the node's old address as the HA cluster's external address.

Syntax:

```
system ha convert ip ip <IPv4 address> netmask <netmask>
system ha convert cidr <CIDR>
```

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)
<CIDR>	IPv4 address in CIRD format (a.b.c.d/e)

Command mode:

Global Configuration mode

Examples:

```
DMC(config)# system ha convert ip ip 9.70.27.245 netmask 255.255.255.0
DMC(config)# system ha convert cidr 9.70.27.245/24
```

See also:

```
show ha-external
```

system ha external delete

HA Cluster External Address Deletion

Remove the HA DMC cluster external address.

Syntax:

```
system ha external delete
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system ha external delete
```

See also:

```
show ha-external
system ha external set
```

system ha external set
Set HA External CIDR Address

Set the DMC cluster's high-availability (HA) external address by specifying an IPv4 address and mask or CIDR designation.

Syntax:

```
system ha external set ip ip <IPv4 address> netmask <netmask>
system ha external set cidr <CIDR>
```

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)
<CIDR>	IPv4 address in CIDR format (a.b.c.d/e)

Command mode:

Global Configuration mode

Examples:

```
DMC(config)# system ha external set ip ip 9.70.27.245 netmask 255.255.255.0
DMC(config)# system ha external set cidr 9.70.27.245/24
```

See also:

```
show ha-external
system ha external delete
```

system ha peer delete

HA Peer Address Deletion

Remove the HA DMC peer's address.

Once the peer address is set, the internal database will automatically restart before processing can continue. When complete, the status will be displayed on the console.

Syntax:

```
system ha peer delete
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system ha peer delete
```

See also:

```
show ha-peer
system ha peer set
```

system ha peer set
Set HA Peer Address

Set the HA DMC peer's address via specifying an IPv4 address and mask or CIDR designation.

Once the peer address is set, the internal database will automatically restart before processing can continue. See status will be displayed on the console.

Syntax:

```
system ha peer set ip ip <IPv4 address> netmask <netmask>
system ha peer set cidr <CIDR>
```

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)
<CIDR>	IPv4 address in CIDR format (a.b.c.d/e)

Command mode:

Global Configuration mode

Examples:

```
DMC(config)# system ha peer set ip ip 9.70.27.54 netmask 255.255.255.0
DMC(config)# system ha peer set cidr 9.70.27.123/24
```

See also:

```
show ha-peer
system ha peer delete
```

system ha start

Start HA

Start the high-availability (HA) feature.

This function will work in the background. When complete, the status will be displayed on the console.

Syntax:

```
system ha start
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system ha start
```

See also:

```
show ha
system ha stop
```

system ha stop

Stop HA

Stop the high-availability (HA) feature.

This function will work in the background. When complete, the status will be displayed on the console.

Syntax:

```
system ha stop
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system ha stop
```

See also:

```
show ha
system ha start
```

system ha synchronization start

Start HA Synchronization

Starts a one-time synchronization of the database from the HA primary node to the HA secondary node.

This function will work in the background. Use the `show ha-synchronization` command to check the status of the synchronization process.

Syntax:

```
system ha synchronization start
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system ha synchronization start
```

See also:

```
show ha-synchronization
```

system ha type set

Set HA Type

Set the high-availability (HA) node as primary or secondary.

Syntax:

```
system ha type set type {primary|secondary|
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system ha type set type primary
```

See also:

```
show ha-type
```

system ipmgmt set

Set DMC IPv4 Address

Set a static DMC address by specifying an IPv4 address and mask or CIDR designation.

Syntax:

```
system ipmgmt set ip addr <IPv4 address> mask <netmask>
system ipmgmt set cidr <CIDR>
```

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)
<CIDR>	IPv4 address in cidr format (a.b.c.d/e)

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system ipmgmt set ip addr 10.10.0.10 mask 255.255.255.0
DMC(config)# system ipmgmt set cidr 10.10.0.10/24
```

See also:

```
show ipmgmt
system ipmgmt set dhcp
```

system ipmgmt set dhcp

Set DMC Dynamic IPv4 Address

Set a dynamic DMC address via DHCP.

Note: Setting the IPv4 address to use DHCP clears the following static configuration information: DMC address, gateway, nameservers, HA peer IPv4 and HA external IPv4 addresses.

Syntax:

```
system ipmgmt set dhcp
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system ipmgmt set dhcp
```

See also:

```
show ipmgmt
system ipmgmt set
```

system nexthop delete

DMC Gateway Address Deletion

Clear the DMC gateway address.

Syntax:

```
system nexthop delete
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system nexthop delete
```

See also:

```
show nexthop
system nexthop set
```

system nexthop set

Set DMC Gateway Address

Set the DMC gateway address via specifying an IPv4 address and mask or CIDR designation.

Syntax:

```
system nexthop set ip addr <IPv4 address> mask <netmask>
system nexthop set cidr <CIDR>
```

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)
<CIDR>	IPv4 address in CIDR format (a.b.c.d/e)

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system nexthop set ip addr 10.10.0.1 mask 255.255.255.0
DMC(config)# system nexthop set cidr 10.10.0.1/24
```

See also:

```
show nexthop
system nexthop delete
```

system password

Change Admin Password

Change the administrator password.

The password length must be at least 6 and no longer than 31 characters.

Syntax:

```
system password
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system password

Enter new admin password: ********
Verify new admin password: ********
Success: admin password changed!
```

system reload

System Reboot

Reboot the DMC. DMC operation is temporarily halted while the software is restarted. When the reboot is complete, the saved configuration is restored and normal operation is resumed.

Syntax:

```
system reload
```

Command mode:

Global Configuration mode

Example:

```
DMC(config)# system reload
Reload DMC [y|n]?: y
Please wait while the DMC is being reloaded!!
```

`terminal-length`

Set Terminal Length

Set the number of lines available on the terminal display.To facilitate reading lengthy output, the display for commands that produce more lines than defined by the terminal length will automatically pause, requiring a keypress before resuming each screen of output.

Syntax:

`terminal-length length <lines>`

Parameters:

<lines>	Number of lines per screen (1-256), or 0 to permit unlimited lines per screen.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# terminal-length length 24
```

See also:

`show terminal-length`

underlay-network add

Underlay IPv4 Subnet Addition

Notifies the DMC regarding a physical (underlay) IPv4 subnet to which TEPs connect. Nexthop indicates the gateway to be used for reaching TEPs outside the network.

DS 5000V Virtual Switches will get this configuration when they first connect to the DMC and will poll the DMC every five minutes for updates.

Only one gateway (next hop) can be configured per address/mask pair. To change a gateway, delete the corresponding configuration and create a new one.

This configuration is needed only if TEPs need to communicate with entities outside their network.

Note: The configuration needs to be made before Dove Switches are configured. (Before the TEP VMKNIC is added to the VDS)

If the configuration needs to be changed after vSwitches have been connected, reset the configuration as follows:

1. Make the appropriate changes on the DMC and ensure they are correct.
2. Remove the TEP VMKNIC on the Dove Switches and reconnect them. This will trigger another relay of information to and from the DMC and this will update the gateway information on the Dove Switches.

Syntax:

`underlay-network add net` *<IPv4 address>* `mask` *<netmask>* `nexthop` *<gateway IPv4>*

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)
<gateway IPv4>	Gateway IPv4 address in dotted decimal notation (a.b.c.d)

Command mode:

Global Configuration mode

Example:

```
DMC(config)# underlay-network add net 10.10.10.0 mask 255.255.255.0 nexthop
10.10.10.254
```

See also:

`underlay-network del`

`show underlay-network`

underlay-network del

Underlay IPv4 Subnet Deletion

Notifies the DMC that an IPv4 address/mask no longer has a gateway (next hop) associated with it. TEPs in the specified network will not be able to communicate with entities outside their network.

vSwitches repeatedly poll the DMC to pick up this configuration and detect changes. For faster discovery, remove the TEP and reconnect it.

Syntax:

```
underlay-network del id <network ID>
```

Parameters:

<network ID>	The target network ID as shown in the `show underlay-network` command.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# underlay-network del id 1
```

See also:

```
underlay-network add
show underlay-network
```

unexport

Unexport a Network Profile

Remove the previously exported network configuration from a remote entity.

If the remote entity is a DS 5000V, the system will attempt to delete the `domain.network.vds-name` profile. If the profile is not found, no error will be reported.

If the profiled ports are in use on the vSwitch, the profile will be marked as deleted and its ports will be blocked. To fully remove the profile, disconnect all VMs from the profile and reissue the `unexport` command, or to restore it, reissue the `export` command.

Syntax:

```
unexport Network_ID <network ID> ip-addr <remote IPv4>
```

Parameters:

<network ID>	Network ID (1-16713214) to export.
<remote IPv4>	IPv4 address of remote target entity.

Command mode:

Global Configuration mode

Example:

```
DMC(config)# unexport Network_ID 10 ip-addr 9.70.27.163
```

See also:

`export`

`show export-list`

update replication_factor
Update Domain Replication Factor

Update the replication factor for a domain. Initially, when a domain is created, its configuration is assigned to two DCS nodes (the minimum) if available. Use this command to specify that the domain configuration be held on additional DCS nodes for resiliency.

The system will attempt to find the requested number of nodes to meet the new replication factor. If the current cluster is not able to meet the new replication factor (for instance, if the replication factor is 4 but only 3 nodes are available), the system with track node availability and perform additional replication when new nodes become available to handle the domain.

Use the `show dcslist` command to display how domains are mapped to DCS nodes at any given time. However, since replication takes place in the background, the time to complete convergence for the expected replication update depends on the availability of nodes and the extent of the domain configuration.

Syntax:

`update replication_factor` <*number of nodes*>

Parameters:

<*number of nodes*> Number of DCS nodes on which to replicate the configuration of the current domain context: minimum 2, maximum 4.

Command mode:

Domain Configuration mode

Example:

```
config:(domain)Corp# update replication_factor 2
```

See also:

`show dcslist`

vlan-gateway add

VLAN Gateway Addition

Associate a VLAN to the overlay network (VNID) in the current domain and network context. This enables VLAN to VNID mapping in the selected gateway appliance.

Syntax:

```
vlan-gateway add dgw_index <gateway ID> vlan_id <VLAN>
```

Parameters:

<gateway ID>	Gateway Index (1-65535).
<VLAN>	Target VLAN ID.

Command mode:

Network Configuration mode

Example:

```
config:(domain)corp:(network)1# vlan-gateway add dgw_index 1 vlan_id 100
```

See also:

```
show vlan-gateway
vlan-gateway del
```

vlan-gateway del

VLAN Gateway Deletion

Delete an existing VLAN gateway within the current domain and network context.

Syntax:

`vlan-gateway del dgw_index <gateway ID>`

Parameters:

<gateway ID>	Target gateway index (1, 65535) as shown in the `show vlan-gateway` command.

Command mode:

Network Configuration mode

Example:

```
config:(domain)corp:(network)1# vlan-gateway del dgw_index 1
```

See also:

`vlan-gateway add`

`show vlan-gateway`

Chapter 9. DSA Show Commands

Once you have logged in to a DOVE Service Appliance (DSA) module, you can view system configuration and statistical information using a variety of CLI `show` commands. The `show` commands are restricted from the User EXEC mode, but most are available globally in all other command modes.

This chapter discusses how to use each of the information-specific CLI `show` commands.

`show cli-timeout`
Show CLI Timeout

Any CLI session will be automatically logged out if idle for the length of time shown.

Syntax:

`show cli-timeout`

Command mode:

Privileged EXEC and above

Example:

```
DSA# show cli-timeout
CLI TIMEOUT 5 min
```

See also:

`system cli timeout`

show config

Show DSA Configuration

Show the current DSA configuration properties. This command consolidates the following information from various other show commands.

- DSA Version
- IPv4 Management Configuration
- Service Appliance Configuration

Syntax:

```
show config
```

Command mode:

Privileged EXEC and above

Example:

```
DSA# show config
Software Version : 1.0.0.130603 Mon Jun  3 15:42:32 PDT 2013

ipmgmt set dhcp

dmc set ipv4 9.70.27.245 port 80
```

show dcs syslog

Show DCS System Log Messages

Show DCS system log messages.

Syntax:

```
show dcs syslog
```

Command mode:

Privileged EXEC and above

Example:

```
DSA# show dcs syslog
DSA Version: 1.0.0.130603 Mon Jun  3 15:42:02 PDT 2013

DSA Version: 1.0.0.130603 Mon Jun  3 15:42:02 PDT 2013

DCS version 1.0.0.130603 Mon Jun  3 15:42:02 PDT 2013

Node IP 127.0.0.1, Port 902
Local DCS Service IP Address: 127.0.0.1
Node IP 127.0.0.1, Port 902
Existing Role File not found [/flash/dcs.role]
DCS: Local Node Inactive
DPS Protocol Handler Stopped
DPS Controller Interface Stopped
Wrote Role 0 to file /flash/dcs.role
DCS Role: Initialized to Inactive
DMC address has not been configured yet
getsockopt SO_RCVBUF returns 2001588984, rcv_size_len 0
setsockopt SO_RCVBUF set to 67108864
Adding Socket 35 to CORE API

DCS Server Started: IP Address <127.0.0.1>, Port <902>
Node IP 9.70.27.54, Port 902
----- Press any key to continue (q to quit) -----
```

show dmc-config

Show DMC Configuration

Show information about the DMC to which the DCS is connected.

Syntax:

```
show dmc-config
```

Command mode:

Privileged EXEC and above

Example:

```
DSA# show dmc-config
        DMC ipv4 : 9.70.27.245
        DMC Port : 80
```

show dsa-version

Show DSA Version

Show DOVE Service Appliance (DMC) software version information.

Syntax:

```
show dsa-version
```

Command mode:

Privileged EXEC and above

Example

```
DSA# show dsa-version
Version: 1.0.0 Mon Apr  8 12:12:23 PDT 2013
```

show ipmgmt

Show IPv4 Management Information

Shows DSA IPv4 address and netmask information.

Syntax:

```
show ipmgmt
```

Command mode:

Privileged EXEC and above

Example:

```
DSA# show ipmgmt
Manage IP Info
================================================================
      Method:                                          Dynamic
          IP:                                      9.70.27.32
        MASK:                                  255.255.255.0
```

See also:

```
ipmgmt set ip
ipmgmt set cidr
ipmgmt set dhcp
```

show ipv4-interfaces
Show IPv4 Interfaces

This command shows all IPv4 interfaces bound to the DSA. This information can be particularly important when configuring gateway (DGW) modules.

Syntax:

```
show ipv4-interfaces
```

Command Mode:

Privileged EXEC and above

Example:

```
DSA# show ipv4-interfaces
            0: 127.0.0.1
            1: 9.70.27.54
```

show system acknowledgement
Show System Acknowledgement & Licensing Information)

Show software licensing information for elements used in the DSA module.

Syntax:

```
show system acknowledgement
```

Command mode:

Privileged EXEC and above

Example:

```
DSA# show system acknowledgement
```

show terminal-length
Show Terminal Length

Show the number of lines displayed per screen. To facilitate reading lengthy output, the display for commands that produce more lines than defined by the terminal length will automatically pause, requiring a keypress before resuming each page of output.

Syntax:

```
show terminal-length
```

Command mode:

Privileged EXEC and above

Example:

```
DMC# show terminal-length
38 lines per screen
```

See also:

```
terminal-length
```

Chapter 10. DSA Configuration Commands

This chapter discusses how to use the individual CLI for making configuration changes.

clear screen

Clear Screen

Clear the terminal screen.

Syntax:

```
clear screen
```

Command mode:

Global Configuration mode

Example:

```
DSA(config)# clear screen
```

clear gwstats

Clear Gateway Statistics

Clear the gateway statistics that are collected by a DSA operating as a DGW node.

Syntax:

```
clear gwstats
```

Command mode:

Global Configuration mode

Example:

```
DSA(config)# clear gwstats
```

cli timeout
CLI Idle Timeout

Sets length of time before CLI times out.

Syntax:

```
cli timeout mins <minutes>
```

Parameters:

<minutes>	Timeout period in minutes.

Command mode:

Global Configuration mode

Example:

```
DSA(config)# cli timeout mins 8
```

See also:

```
show cli-timeout
```

dmc set ip

Bind DSA to DMC

Define the IPv4 address of the DMC to which this DSA will register.

Syntax:

```
dmc set ip addr <IPv4 address> [mask <netmask>]
```

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)

Command mode:

Global Configuration mode

Example:

```
DSA(config)# dmc set ip addr 10.10.0.10 mask 255.255.255.0
```

dsa-upgrade

Upgrade DSA Software Image

Upgrade the DSA software image. The new image file must be accessible to the DSA. Once upgraded, the DSA will automatically reboot in order to run the new image. You can verify the upgrade by using the `show dsa-version` command.

Syntax:

`dsa-upgrade url` <*image URL*>

Parameters:

<*image URL*> URL (1 to 128 characters) for the DSA software image file.

Command mode:

Global Configuration mode

Example:

```
DSA(config)# system dmc-upgrade url
ftp://9.111.86.13/xyl/ibm-sdn-dsa-upgrade-1.0.0.img
Please wait while the DSA Image is being upgraded!!
DSA(config)#
```

See also:

`show dsa-version`

`reload`

`exit`

Exit the Current Context Mode

Exit from a context sub-mode and return to the parent mode. If already at the top level, exit from the command line interface and log out.

Syntax:

`exit`

Command mode:

All

Example:

```
DSA(config)# exit
DSA# exit
DSA>
```

See also:

`quit`

`find`

Find Command Syntax

List the commands available in the current mode.

Syntax:

```
find
```

Command mode:

All

ipmgmt set

Set DSA Static IPv4 Address

Set a static DSA address by specifying an IPv4 address and netmask or CIDR designation.

Syntax:

```
ipmgmt set ip addr <IPv4 address> mask <netmask>
ipmgmt set cidr <CIDR>
```

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)
<CIDR>	IPv4 address in CIDR format (a.b.c.d/e)

Command mode:

Global Configuration mode

Examples:

```
DSA(config)# ipmgmt set ip addr 10.10.0.10 mask 255.255.255.0
DSA(config)# ipmgmt set cidr 10.10.0.10/24
```

See also:

```
show ipmgmt
ipmgmt set dhcp
```

ipmgmt set dhcp
Set DSA Dynamic IPv4 Address

Set a dynamic DSA address via DHCP.

Note: Setting the IPv4 address to use DHCP clears the following static DSA IPv4 address and gateway.

Syntax:

```
ipmgmt set dhcp
```

Command mode:

Global Configuration mode

Example:

```
DSA(config)# ipmgmt set dhcp
```

See also:

```
show ipmgmt
ipmgmt set
```

ipmgmt set nexthop ip

Set DSA Gateway IPv4 Address

Set the DSA gateway address by specifying a static IPv4 address and netmask.

Syntax:

```
ipmgmt set nexthop ip addr <IPv4 address> mask <netmask>
```

Parameters:

<IPv4 address>	IPv4 address in dotted decimal notation (a.b.c.d)
<netmask>	IPv4 netmask in dotted decimal notation (a.b.c.d)

Command mode:

Global Configuration mode

Example:

```
DSA(config)# ipmgmt set nexthop ip addr 10.10.0.1 mask 255.255.255.0
```

`ping`

Ping Test Network Connection

Use the ping utility to test network connectivity.

Syntax:

`ping dst` <*destination IPv4*> `[src` <*source IPv4*>`]`

Parameters:

<*destination IPv4*> Destination IPv4 address.

<*source IPv4*> Optional source IPv4 address.

Command mode:

All

Example:

```
DSA# ping dst 9.0.130.50
PING 9.0.130.50 (9.0.130.50): 56 data bytes
64 bytes from 9.0.130.50: seq=0 ttl=115 time=76.719 ms
64 bytes from 9.0.130.50: seq=1 ttl=115 time=76.528 ms
64 bytes from 9.0.130.50: seq=2 ttl=115 time=76.730 ms
64 bytes from 9.0.130.50: seq=3 ttl=115 time=78.763 ms
--- 9.0.130.50 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 76.528/77.185/78.763 ms
```

`quit`

Quit the ICSLI Session

Exit from the CLI and log out.

Syntax

`quit`

Command mode:

All

Example:

```
DSA(config)# quit
```

See also:

`exit`

password

Change DSA Admin Password

Change the DSA administrator password.

The password length must be at least 6 and no longer than 31 characters.

Syntax:

```
password
```

Command mode:

Global Configuration mode

Example:

```
DSA(config)# password

Enter new admin password: ********
Verify new admin password: ********
Success: admin password changed!
```

`reload`

Reset and Reboot the DSA

Reset and reboot the DSA module.

Syntax:

`reload`

Command mode:

Global Configuration mode

Example:

```
DSA(config)# reload
Reload DMC [y|n]?: y
Please wait while the DSA is being reloaded!!
```

`show`

Show Information

You can view DSA configuration and statistical information using a variety of `show` commands. For details, see “DSA Show Commands” on page 179.

`terminal-length`

Set Terminal Length

Set the number of lines available on the terminal display. To facilitate reading lengthy output, the display for commands that produce more lines than defined by the terminal length will automatically pause, requiring a keypress before resuming each screen of output.

Syntax:

`terminal-length length <lines>`

Parameters:

<lines>	Number of lines per screen (1-256), or 0 to permit unlimited lines per screen.

Command mode:

Global Configuration mode

Example:

```
DSA(config)# terminal-length length 24
```

See also:

`show terminal-length`

Part 3: Appendices

Appendix A. Known Issues

The following caveats and limitations were known to exist at the time of initial release for SDN VE version 1.0.0 and may change as new software becomes available. For the most up-to-date list of known issues, refer to the readme file that is made available with each software update.

External Gateways

- IPv4 addresses in the External Gateway (EGW) pool cannot be modified. Only additions and delete are supported. (ID: 71464)
- Communication between two Domains is not possible if both Domains map to the same EGW. (ID: 71513)
- EGW failover is not triggered when connectivity with the next-hop or 5000V is disrupted.
- When EGW failover occurs, existing NAT sessions are not failed restored.

High Availability

- After a failover event, if show ha output indicates a connection status of "`not configured`" in the primary DMC, manual intervention via the `system ha synchronization start` command is required. (ID: 71755)
- If the HA system remains in failure mode long enough, the primary DMC will revert to "standalone" (non-HA) mode to avoid system conflicts. Recovering from this state requires manual intervention to stop HA (`system ha stop`), resynchronize (`system ha synchronization start`), verify (`show ha-synchronization`), and restart (`system ha start`).

IP Addresses

- If an IPv4 address is removed from a VM, it is not unregistered if there is continuous traffic for it. (ID: 71502)
- IPv4 address conflict on the same host and same virtual network results in loss of communication. (ID: 71560)
- If a VM's IPv4 address is changed, the IPv4 address is not unregistered if there is continued traffic to another VM on same host. (ID: 71604)
- IPv6 addresses are not presently supported.

Management

- Internal management and control channels are currently not authenticated. (ID: 69071)
- Repeated, heavy use of administrative commands (such as `system ha start` and `system ha stop`) can saturate the system database and is not recommended. (ID: 71770)

Protocols and Traffic

- IGMP reports are not sent to DGW appliances. Manual multicast configuration is needed to overcome this limitation. (ID: 69204)
- Enabling port mirroring results in tagged packets being incorrectly delivered to an untagged destination. (ID: 70374)
- Jumbo Frame traffic is not supported by the 5000V switch or DGWs. (ID: 71498)

- Tunnel End-Points (TEPs) cannot be assigned to a user defined VLAN. (ID: 71686)
- FTP server passive mode in networks configured as `dedicated` cannot be accessed via the EGW. (ID: 71754)

Virtual Machines (VMs)

- VM that do not participate in network traffic may not appear in the show endpoints output. (ID: 69562)
- Addition of a network adapter to a functioning VM disrupts connectivity of existing virtual ports from that VM (ID: 71465)
- If VMs are not restarted after the host server is power cycled or rebooted, entries for those VMs will still appear in the show endpoints output. (ID: 71538)
- VMs connected to the SDN VE virtual network through the 5000V vDS may lose connectivity after Storage VMotion. (ID: 71723)

Virtual Switching

- Interface level configuration of ports in the 5000V vDS are not supported, though not explicitly disallowed in the CLI. (ID: 71003)
- Only one 5000V vDS per host server is supported for SDN VE use. (ID: 71750)

Appendix B. Getting Help & Technical Assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before You Call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your system.
- Go to the IBM support website at http://www.ibm.com/systems/support/ to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the Documentation

Information about your IBM system and pre-installed software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, ReadMe files, and Help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/systems/support/ and follow the instructions. Also, some documents are available through the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Getting Help and Information on the World Wide Web

On the World Wide Web, the IBM website has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x® and xSeries® information is http://www.ibm.com/systems/x/. The address for IBM BladeCenter information is http://www.ibm.com/systems/bladecenter/. The address for IBM IntelliStation® information is http://www.ibm.com/intellistation/.

You can find service information for IBM systems and optional devices at http://www.ibm.com/systems/support/.

Software Service and Support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and x Series servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, see http://www.ibm.com/services/, or see http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware Service and Support

You can receive hardware service through your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/partnerworld/ and click **Find Business Partners** on the right side of the page. For IBM support telephone numbers, see http://www.ibm.com/planetwide/. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan Product Service

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Appendix C. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important Notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from IBM.

Maximum memory might require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate Contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the devices that run the software described in this document. Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Documentation Format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

Information Development
IBM Corporation
205/A0153039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

In the request, be sure to include the publication title.

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.