BROCADE VDX Configuration Cheat sheet 1/2

Connecting via Console Cable

Connect the serial port with a straight through cable to the serial port of a PC. Serial parameters are : 9600Baud, 8 bits, no parity, 1 stop bit and no flow control.

Setting the switch IP address

When using DHCP, the Brocade VDX switches obtain the IP address, subnet mask, and default gateway address from the DHCP server. The DHCP client can only connect to a DHCP server that is on the same subnet as the switch. If your DHCP server is not on the same subnet as the Brocade VDX 6740, use a static IP address.

To set an IPv4 IP address using **DHCP**, complete the following steps.

1. Log in to the switch using the admin account.
2. Configure the management interface with the following command:

```
switch(config)# interface Management 1/0
```

3. Configure the IP address using the following command:

```
switch(config-Management-1/0)# ip address dhcp
```

Complete the following steps to set a **static IP address**.

1. Log in to the switch using the default password (the default password is password).
2. Use the ip address command to set the Ethernet IP address. You should also enter a gateway address as well.

```
switch(config)# interface Management 1/0
switch(config-Management-1/0)# no ip address dhcp
switch(config-Management-1/0)# ip address 10.24.85.81/20
```

To set up a default gateway, add an ip route in rbridge mode.

```
switch(config-rbridge-id-10)# ip route 0.0.0.0/0 10.24.80.1
switch# copy running-config startup-config
```

3. To display the configuration, use the show running-config interface Management command.

```
switch# show running-config interface Management 1/0
        interface Management 1/0
        no ip address dhcp
        ip address 10.24.85.81/20
```

Changing the RBridge ID

If you are going to have more than one switch in the same fabric, each switch must have a unique RBridge ID. The default RBridge ID for any Brocade VDX is 1. Use the vcs rbridge-id [rbridge-id] command to change the default RBridge ID. You should be in privileged EXEC mode to run the command. If you have made any other configuration changes you want to persist, be sure to save your running configuration to the startup configuration before running the vcs rbridge-id command as this command reboots the switch.

Enter the **vcs rbridge-id** [rbridge-id] command.

```
switch# vcs rbridge-id 2
This operation will change the configuration to default and
reboot the switch. Do you want to continue? [y/n]:y
```

When the confirmation question appears, answer Y. The reply to the command will include a line about the setting of the RBridge ID.

```
Successfully set rbridge-id.
```

Changing the VCS ID

If you are going to have more than one VCS fabric*, each fabric must have a unique VCS ID. The default VCS ID for any VCS fabric is 1. Use the vcs vcs -id [ID] command to change the default VCS ID. You should be in privileged EXEC mode to run the command. If you have made any other configuration changes you want to persist, be sure to save your running configuration to the startup configuration before running the vcs vcsid command as this command reboots the switch.

Enter the **vcs vcsid** [ID] command.

```
switch# vcs vcsid 2
This operation will change the configuration to default and
reboot the switch. Do you want to continue? [y/n]:y
```

When the confirmation question appears, answer Y.

The reply to the command will include a line about the setting of the VCS ID.

```
Successfully set vcsid.
```

requires extra license

Changing the default passwords

Default administrative account names and passwords

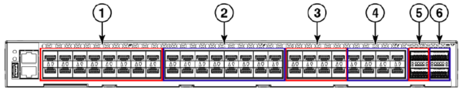
Account type	Login name	Password
Administrative	admin	password
User account (read-only)	user	password

When you change the default account password after you log in for the first time, only the default password rule is in effect. The rule specifies a minimum password length of eight characters.

1. Enter the configure terminal command to enter global configu ration mode.
2. Enter the username command followed by the account name and the password parameter.
3. When prompted, enter the new password. and press Enter.

```
Switch# configure terminal
Entering configuration mode terminal
switch(config)# username admin password
```

Inter-Switch Link trunks (ISL)



1	Trunk Group 1 - 1/10 GbE SFP ports 1-16	4	Trunk group 4 - 1/10 GbE SFP ports 41-48
2	Trunk Group 2 - 1/10 GbE SFP ports 17-32	5	Trunk Group 3A - 40 GbE QSFP ports 49-50
3	Trunk Group 3 - 1/10 GbE SFP ports 33-40	6	Trunk Group 4A - 40 GbE QSFP ports 51-52

In VCS mode, unless specifically disabled, inter-switch link (ISL) Brocade trunking between adjacent switches is automatic. All ports must be in the same port group and must be configured at the same speed. There is a limit of sixteen ports per trunk group. No separate licensing is required. On the Brocade VDX 6740T and VDX 6740T-1G, ports in groups 3, as well as port groups 4, cannot be trunked together. However, these ports can be trunked on the VDX 6740 when the 40 GbE QSFP ports are configured in breakout mode. VDX 6740T-1G 1GbE ports cannot be trunked.

Configuring Edge Loop Detection (ELD)

Setting global ELD parameters for a VCS Fabric cluster

The values in this example configure the Brocade VCS Fabric cluster to detect and break loops on receipt of 5 PDUs. Because the PDU interval is set to 2000 ms (2 seconds), any loop breaks after 10 seconds. The selected port will remain disabled for 24 hours, after which it is automatically re-enabled.

1. Log in to any switch in a Brocade VCS Fabric cluster.
2. Enter the **protocol edge-loop-detection**

```
switch(config)# protocol edge-loop-detection
```

3. Enter the **pdu-rx-limit** *number* to set the n# (1<n°<5, def=1) of PDUs that will be received before breaking the Layer 2 loop.

```
switch(config-eld)# pdu-rx-limit 5
```

4. Enter **hello-interval** *number* to set the interval between PDUs. (100ms < *number < 5000ms, def 1000ms)*

```
switch(config-eld)# hello-interval 2000
```

5. Enter **mac-refresh** *number* to flush MAC addresses at a specified interval on either the cluster or port to remove any MAC inconsistencies in your system. (60s < number<300s)(all/port)

```
switch(config-eld)# mac refresh 100 all
```

6. Enter **shutdown-time** *number* to set the number of minutes after which the shutdown port is re-enabled. (10min <number<1440 min, def 0)

```
switch(config-eld)# shutdown-time 1440
```

Setting interface parameters on a port

Perform this procedure for every port you want to be monitored by ELD.

1. Log in to any switch in a VCS Fabric cluster.
2. Enter the **interface** command to select the *rbridge-id/slot/port* for which you want to enable edge-loop detection.
3. Enter the **edge-loop-detection vlan** command to specify the VLAN you want ELD to monitor on this port.
4. Enter **edge-loop-detection port-priority** to specify the ELD port priority of the specified port for the selected VLAN.

NOTE

The priority range of values is from 0 through 255. A port with priority 0 means that shutdown for this port is disabled. The default value port priority is 128 .

Setting the ELD port priority on two port/VLAN pairs

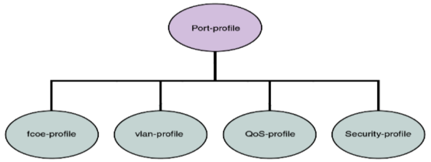
This example sets the ELD port priority on two port/VLAN pairs: port 1/0/7 VLAN 10 and port 4/0/6 VLAN 10.

If both these ports are detected in the same loop, ELD shuts down port 4/0/6 when the pdu-rx-limit for the VCS Fabric cluster is reached. Port 4/0/6 is chosen for shut down because it has been assigned the lower priority (higher number) then port 1/0/7.

```
switch(config)# interface TenGigabitEthernet 1/0/7
switch(conf-if-te-1/0/7)# edge-loop-detection vlan 10
```

Configuring Auto Migrating Port Profile

Server virtualization infrastructure associates a server-side Virtual Ethernet Bridge (VEB) port-profile with each Ethernet MAC address used by a virtual machine (VM) to access the network through a VEB port. The Auto Migrating Port Profile (**AMPP**) feature provides advanced controls for maintaining and migrating these port-profile associations when a VM migrates



Configuring a new port-profile

1. Configure the physical interface, LAG, or vLAG as a port-profile port.

```
switch(if-te-2/0/1)# port-profile-port
```

2. Create and configure a new port-profile name.

```
switch# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
switch(config)# port-profile vm1-port-profile
switch(config-port-profile-vm1-port-profile)# vlan-profile
switch(config-pp-vlan)# switchport
switch(config-pp-vlan)# switchport mode trunk
switch(config-pp-vlan)# switchport trunk native-vlan 300
switch(config-pp-vlan)# switchport trunk allowed vlan add 300
```

3. Exit VLAN profile configuration mode.

```
switch(config-pp-vlan)# exit
```

4. Activate the profile.

```
switch(config)# port-profile vm1-port-profile activate
```

5. Associate the profile to the MAC address for each host.

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

Configuring VLAN profiles

The VLAN profile defines the VLAN membership of the overall port-profile, which includes both the tagged and untagged VLANs.

1. De-activate the port-profile before modifying the VLAN profile.

```
switch(config)# no port-profile vm1-port-profile activate
```

2. Enter VLAN profile configuration mode.

```
switch(config)# port-profile vm1-port-profile
switch(config-port-profile-vm1-port-profile)# vlan-profile
```

3. Use the switchport command to change the mode to Layer 2

```
switch(config-pp-vlan)# switchport
```

4. Access the VLAN profile mode for the correct VLAN.

```
switch(config-pp-vlan)# switchport access vlan 200
```

5. Enter trunk configuration mode.

```
switch(config-pp-vlan)# switchport mode trunk
```

6. Configure the trunk mode for the allowed VLAN IDs.

```
switch(config-pp-vlan)# switchport trunk allowed vlan add 10, 20, 30-40
```

7. Configure the trunk mode to be a native VLAN.

```
switch(config-pp-vlan)# switchport trunk native-vlan 300
```

8. Exit VLAN profile configuration mode.

```
switch(config-pp-vlan)# exit
```

9. Activate the profile.

```
switch(config)# port-profile vm1-port-profile activate
```

10. Associate the profile to the MAC address for each host.

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
...
```

BROCADE VDX Configuration Cheat sheet 1/2

Configuring Auto Migrating Port Profile

Configuring QoS profiles

QoS profiles define the following values:

- Incoming 802.1p priority is set to internal queue priority. If the port is in
- QoS untrusted mode, all incoming priorities will be mapped to default best effort priority.
- Incoming priority is set to outgoing priority.
- Mapping of incoming priorities is set to strict or WRR traffic classes.
- Enabling of flow control on a strict or a WRR traffic class.

The QoS profile has two flavors: CEE QoS and Ethernet QoS. Server side ports typically are carrying converged traffic. The priority-mapping-table can support features provided by the Cisco Modular Quality of Service (MQC) provisioning mode to bring partial Converged Enhanced Ethernet (CEE) map content into an MQC class

To configure the QoS profile, perform the following steps.

1. Deactivate the port-profile before modifying the VLAN profile.

```
switch(config)# no port-profile vm1-port-profile activate
```

2. Enter QoS profile mode.

```
switch(config)# port-profile vm1-port-profile
switch(config-port-profile-vm1-port-profile)# qos-profile
switch(config-qos-profile)#
```

3. Apply the CEE map.

```
switch(config-qos-profile)# cee default
```

4. Apply a map to the profile. You can do either of the following:

• Apply the existing CoS-to-CoS mutation map.

```
switch(config-qos-profile)# qos cos-mutation vm1-cos2cos-map
```

• Apply the existing CoS-to-Traffic-Class map.

```
switch(config-qos-profile)# qos cos-traffic-class vm1-cos2traffic-map
```

5. Enable pause generation for each CoS.

```
switch(config-qos-profile)# qos flowcontrol tx on rx on
```

6. Exit QoS profile mode.

```
switch(config-qos-profile)# exit
```

7. Activate the profile.

```
switch(config)# port-profile vm1-port-profile activate
```

8. Associate the profile to the MAC address for each host.

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
...
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

Configuring security profiles

A security profile defines all the security rules needed for the server port. A typical security profile contains attributes for MAC-based and IP-based standard and extended ACLs. Security profiles are applied to the ACLs based on the profile or PolicyID. Therefore, multiple security profiles can be applied to the same profiled port.

To configure the security profile, perform the following steps.

1. Deactivate the port-profile before modifying the security profile.

```
switch(config)# no port-profile vm1-port-profile activate
```

2. Enter security profile configuration mode.

```
switch(config)# port-profile vm1-port-profile
switch(config-pp)# security-profile
switch(config-pp-security)#
```

3. Modify the ACL security attributes.

4. Apply the ACL to the security profile.

```
switch(config-pp-security)# mac access-group vm1-acl in
```

5. Exit security profile configuration mode.

```
switch(config-pp-security)# exit
```

6. Activate the profile.

```
switch(config)# port-profile vm1-port-profile activate
```

7. Associate the profile to the MAC address for each host.

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
...
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

Configuring FCoE profiles

Both default and nondefault port profies are supported. Refer to FCoE on page 37 for details.

Note

Before a port profile can be modified, no interfaces can have a port-profile-port configuration. In the absence of the FCoE profile in the default AMPP profile, you can configure FCoE on a per-interface basis, based on the profiled ports.

To configure a default FCoE profile globally, perform the following steps.

1. Enter port-profile configuration mode.

```
switch(config)# port-profile default
```

2. Enter FCoE-profile configuration mode.

```
switch(config-port-profile-default)# fcoe-profile
```

3. Activate the FCoE port profile.

An FCoE map cannot be applied on interfaces that already have a CEE map applied to it.

```
switch(config-fcoe-profile)# fcoeport default
```

Creating a port-profile-port

To create a port-profile-port, perform the following steps in global configuration mode.

1. Activate the interface configuration mode for the interface you wish to modify.

The following example activates the mode for the 10-gigabit Ethernet interface in slot 0/port 0.

```
switch(config)# interface tengigabitethernet 1/0/1
```

2. Configure port-profile-port on the physical interface.

```
switch(conf-int-te-1/0/1)# port-profile-port
```

Deleting a port-profile-port

To delete a port-profile-port, perform the following steps in global configuration mode.

1. Activate the interface configuration mode for the interface you wish to modify.

The following example activates the mode for the 10-gigabit Ethernet interface in slot 0/port 0.

```
switch(config)# interface tengigabitethernet 1/0/1
```

2. Unconfigure port-profile-port on the physical interface.

```
switch(conf-int-te-1/0/1)# no port-profile-port
switch(conf-int-te-1/0/1)# no shutdown
```

Deleting a port-profile

To delete a port-profile, perform the following steps in privileged EXEC mode.

1. Enter global configuration mode.

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

2. Deactivate the port-profile.

```
switch(config)# no port-profile vm1-port-profile activate
```

3. Use the **no** form of the **port-profile** command to delete the custom profile. You cannot delete the default port-profile.

```
switch(config)# no port-profile vm1-port-profile
```

Fibre Channel Ports overview

- E_Port: Can be used to connect only to an EX_Port on a FC SAN with Fibre Channel Routing configured.
- F_Port:
  - Supports FC target connectivity (standards based F_Port).
  - Supports bidirectional traffic internally from VF_Port, or internal ISL port.
- Auto (G_Port) — This is the default.
- N_port:
  - Default port type in Access Gateway mode
  - Available in Access Gateway mode only
  - Supports bidirectional traffic internally from VF_Port.
  - External connection to F_Port on a FC SAN
- VF_port:
  - For FCoE initiator or target connectivity.
  - Supports bidirectional traffic internally to E_Port, F_Port, VF_Port (all in FCF mode), and N_Port (in AG mode).

Configuring Fibre Channel Ports

Flexport overview

The FlexPort feature allows up to 32 ports to transmit data as either 10G Ethernet or Fibre Channel, and to be changed from one type to the other without requiring a reboot. These ports are grouped together as connector groups. Connector groups share common speed and protocol type properties. The settings allow any port within each connector group to operate as either Ethernet or Fibre Channel ports, and support the appropriate optic transceivers. The Fibre Channel ports must be running any supported 8-Gbps or 16-Gbps Brocade FC transceivers. The default setting is Ethernet.

Speed combinations allowed per connector-group are:

- LowMixed - 2/4/8G Fibre Channel, and Ethernet speeds (default)
- HighMixed - 16G Fibre Channel, and Ethernet speeds
- FibreChannel - 2/4/8/16G Fibre Channel (Only if all eight ports are already set as Fibre Channel type)

For the currently supported platforms, the connector-group numbers range from 1 through 6. They are related directly to the ports as numbered on each platform. The connector-group numbers that are allowed to be changed and their associated port numbers are shown in the table below.

Platform	Port Number range	Connector group
VDX 6740	1-8	1
	17-24	3
	33-40	5
	41-48	6

Configuring FlexPort

The FlexPort feature allows up to 32 ports to transmit either Ethernet or Fibre Channel. The FlexPort feature is set to Ethernet by default. You should only need to perform this task to switch to Fibre Channel, or back to Ethernet.

1. Enter hardware configuration mode.

```
switch(config)#hardware
switch(config-hw)#
```

2. Enter FlexPort configuration mode for the switch. This command config ures FlexPort 5 on RBridge ID 1. FlexPort 5 is part of connector group 1 on the VDX 6740.

```
switch(config-hw)# flexport 1/0/5
switch(conf-hw-flex-1/0/5)#
```

3. Set the FlexPort type to Fibre Channel.

```
switch(conf-hw-flex-1/0/5)# type FibreChannel
```

4. Optionally, you may adjust the speed for the connector group. For example, if you want the connector group 1 to function at 16Gbps speed:

```
switch(conf-hw-flex-1/0/5)# connector-group 1/0/1
switch(config-connector-group-1/0/1)# speed HighMixed
```

5. Repeat these steps for additional switches as needed.

6. Confirm the FlexPort configuration with the show running-config hard ware flexport command.

```
switch# show running-config hardware flexport
Hardware
  flexport 1/0/1
      type FibreChannel
!
Hardware
   flexport 1/0/5
       type FibreChannel
!
connector-group 1/0/1
  speed HighMixed
!
```

Configuring Zoning

A zone is made up of one or more zone members. Each zone member can be a device, a port, or an alias. If the zone member is a device, it must be identified by its Node World Wide Name (node WWN). If it is a port, it must be identified by its Port World Wide Name (port WWN). Port WWNs and node WWNs can be mixed in the same zone. For LSAN zones, only port WWNs can be used. World Wide Names are specified as 8-byte (16-digit) hexadecimal numbers, separated by colons (:) for example, 10:00:00:90:69:00:00:8a

Creating a zone

Enter the **show name-server detail** command to obtain the WWNs of servers and targets available in the VCS Fabric.

Example of creating a zone with two members, a WWN and an alias:

```
switch# show name-server detail
PID: 012100
Port Name: 10:00:00:05:1E:ED:95:38
Node Name: 20:00:00:05:1E:ED:95:38
    (output truncated)

switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration zone zone1
switch(config-zone-zone1)# member-entry
20:00:00:05:1E:ED:95:38;alias2
switch(config-zone-zone1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

Adding a member to a zone

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration zone zone1
switch(config-zone-zone1)# member-entry
50:05:07:61:00:1b:62:ed;50:05:07:61:00:09:20:b4;alias3
switch(config-zone-zone1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

Removing a member to a zone

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration zone zone1
switch(config-zone-zone1)# no member-entry 50:05:07:61:00:09:20:b4
switch(config-zone-zone1)# no member-entry alias3
switch(config-zone-zone1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

Deleting a zone

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no zoning defined-configuration zone zone2
switch(config)# zoning enabled-configuration cfg-action cfg-save
Updating flash ...
switch(config)# exit
switch# show running-config zoning defined-configuration
zoning defined-configuration zone zone1
member-entry 10:00:00:00:00:00:00:01
```

Creating an alias

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# member-entry 10:00:00:00:00:00:00:01
switch(config-alias-alias1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

BROCADE VDX Configuration Cheat sheet 2/2

VMWare vCenter integration

Overview

The VMware vCenter and Brocade Network OS integration supported in VCS Fabric mode enables you to discover VMware ESX servers managed by a vCenter server. VMware's server hosts (ESX servers) are connected directly to the physical switches through the switch ports (edge ports in VCS Fabric mode). The server hosts implement a virtual switch (vSwitch), which is used to provide connections to the VMs. The fundamental requirement for the vCenter and Network OS integration is the IP-level management connectivity of the vCenter Server 4.0 version and later with the VDX switches. In addition to creating the VMs, the server administrator associates the VMs with distributed virtual switches, distributed virtual port groups, standard virtual switches (vSwitches) and standard port groups. The vCenter automatically generates some of the VM properties (such as the MAC address), and some properties must be configured (such as the VLAN properties).

NOTE

The Network OS integration requires vCenter versions 4.0, 4.1, 5.1 or 5.5.

vCenter guidelines and restrictions

- Special characters in the port group names are replaced with the URL -encoded values.
- Standard port groups with the same name that reside in different ESX/ESXi hosts must have identical VLAN settings across all hosts.
- For all vCenter port groups, Network OS automatically creates a port profile with the following format: auto-vcenter_name-datacenter_ID -port-group-name.
- Network OS supports vCenter discovery that is based on events.
- Network OS supports LLDP and QoS (IEEE 8021.p) for distributed virtual switches (dvSwitches).
- CDP/LLDP-receiving interface ports must not have any conflicting configurations on the interface that prevent them from being in a port-profiled mode.
- An interface is prevented from becoming a port-profile-port only when conflicting switchport, QoS,and security configurations reside on the interface. An FCoE configuration on the interface does not prevent a port-profile-port configuration.
- Before configuring a vCenter in the fabric, remove all the manually created port profiles that have vCenter inventory MAC associations.
- Up to four vCenter configurations are supported per fabric, with support for multiple data centers.
- Duplicate vCenter asset values are not supported, such as duplicate MAC addresses and duplicate Host names.

vCenter configuration

Step 1: Enabling QoS

You must edit the network resource pool settings and set QoS priorities. Refer to the latest VMware vSphere Networking documentation.

Step 2: Enabling CDP/LLDP

In order for an Ethernet Fabric to detect the ESX/ESXi hosts, you must first enable Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) on all the virtual switches (vSwitches) and distributed vSwitches (dvSwitches) in the vCenter Inventory.

For more information, refer to the VMware KB article 1003885.

Enabling CDP/LLDP on vSwitches

1. Login as root to the ESX/ESXi Host.
2. Use the following command to verify the current CDP/LLDP settings.

```
[root@server root]# esxcfg-vswitch -b vSwitch1
```

3. Use the following command to enable CDP/LLDP for a given virtual switch. Possible values here are advertise or both.

```
[root@server root]# esxcfg-vswitch -B both vSwitch1
```

Enabling CDP/LLDP on dvSwitches

1. Connect to the vCenter server by using the vSphere Client.
2. On the vCenter Server home page, click Networking.
3. Right-click the distributed virtual switches and click Edit Settings.
4. Select Advanced under Properties.
5. Change the CDP/LLDP settings.

Step 3: Adding and activating the vCenter

Adding the vCenter

1. Enter the vcenter command with the name, URL, user name, and password of the vCenter.

```
switch(config)# vcenter myvcenter url https://10.2.2.2 username user password pass
```

2. An invalid state or condition of a vCenter can cause the deletion of all auto-port-profiles in a system. To prevent this from happening, configure the ignore-delete-all-response operand of the vcenter command to ignore the "delete-all" responses from the vCenter.

```
switch# vcenter MYVC discover ignore-delete-all-response 5
```

Activating the vCenter

After adding the vCenter, you must activate the configured vCenter instance.

1. Enter the configure terminal command.
2. Enter the vcenter command to activate the vCenter.

```
switch(config)# vcenter myvcenter activate
```

Immediately following first-time vCenter activation, the Network OS starts the virtual asset discovery process.

```
switch# show vnetwork vcenter status
```

Discovery timer interval

By default, Network OS queries the vCenter updates every thirty minutes. If any virtual assets are modified (for example, adding or deleting virtual machines (VMs), or changing VLANs), Network OS detects those changes and automatically reconfigures the Ethernet Fabric during the next periodic rediscovery attempt.

Use the vcenter interval command to manually change the default timer interval value to suit the individual environment needs.

```
switch(config)# vcenter myvcenter interval ?
Possible completions:
<NUMBER:0-1440> Timer Interval in Minutes (default = 30)
```

Adding the vCenter

User-triggered vCenter discovery

The discovery of virtual assets from the vCenter occurs during one of the following circumstances:

- When a switch boots up.
- When a new vCenter is configured on the VDX switch and activated
- When the discovery is explicitly initiated with the CLI.

To explicitly initate vCenter discovery:

```
switch(config)# vcenter MYVC discover ignore-delete-all-response 5
switch(config)# exit
switch#
switch# vnetwork vcenter myvcenter discover
```

Viewing the discovered virtual assets

Enter one of the following show vnetwork asset commands:

- show vnetwork datacenter vcenter vcenter_name
- show vnetwork dvpgs datacenter datacenter_id vcenter vcenter_name
- show vnetwork dvs datacenter datacenter_id vcenter vcenter_name
- show vnetwork hosts datacenter datacenter_id vcenter vcenter_name
- show vnetwork pgs datacenter datacenter_id vcenter vcenter_name
- show vnetwork vcenter status
- show vnetwork vmpolicy macaddr datacenterdatacenter_id vcenter vcenter_name
- show vnetwork vms datacenter datacenter_id vcenter vcenter_name
- show vnetwork vss datacenter datacenter_id vcenter vcenter_name

where:

- dvpgs — Displays discovered distributed virtual port groups.
- dvs — Displays discovered distributed virtual switches.
- hosts — Displays discovered hosts.
- pgs — Displays discovered standard port groups.
- vcenter status — Displays configured vCenter status.
- vmpolicy — Displays the network policies
- vms — Displays discovered virtual machines (VMs).
- vss — Displays discovered standard virtual switches.