HP Virtual Connect Manager Command Line Interface for c-Class BladeSystem Version 3.00 User Guide

for HP Integrity BL8x0c i2 Series Server Blades

Part Number 592319-002
June 2010 (Second Edition)

Intended audience

This document is for the person who installs, administers, and troubleshoots servers and storage systems. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Contents

Introduction

What's New

This version of the command line interface user guide contains the following changes:

- Support for the HP Integrity BL8x0c i2 Series Servers

  This server is a multi-blade server, which has one bay identified as the monarch bay. All operations on the multi-blade server are done on the monarch bay, although the operation, such as power on or assigning a profile, affects the entire multi-blade server.

- Removed the `update firmware` command.

  To update firmware, use the HP BladeSystem c-Class Virtual Connect Support Utility. For more information on installing the firmware, see the HP BladeSystem c-Class Virtual Connect Support Utility documentation on the HP website (http://www.hp.com/go/bladesystem/documentation).

- New managed element: statistics

Virtual Connect overview

Virtual Connect is a set of interconnect modules and embedded software for HP BladeSystem c-Class enclosures that simplifies the setup and administration of server connections. HP Virtual Connect includes the following components:

- HP 1/10Gb Virtual Connect Ethernet Module for c-Class BladeSystem
- HP 1/10Gb-F Virtual Connect Ethernet Module for the c-Class BladeSystem
- HP Virtual Connect Flex-10 10Gb Ethernet Module for BladeSystem c-Class
- HP 4Gb Virtual Connect Fibre Channel Module for c-Class BladeSystem
- HP Virtual Connect 4Gb Fibre Channel Module for BladeSystem c-Class (enhanced NPIV)
- HP Virtual Connect 8Gb 24-Port Fibre Channel Module for BladeSystem c-Class
- HP Virtual Connect 8Gb 20-Port Fibre Channel Module for BladeSystem c-Class
- HP Virtual Connect Manager

Virtual Connect implements server edge virtualization so that server administrators can upgrade, replace, or move server blades within their enclosures without changes being visible to the external LAN and SAN environments.

The Virtual Connect Manager is embedded on the Virtual Connect Ethernet module. Users access VCM through a web-based GUI or CLI. The Onboard Administrator provides a web link to the GUI. Use an SSH session to establish a console connection to the CLI.

The Virtual Connect Ethernet modules and the Virtual Connect FC modules support the HP BladeSystem c7000 Enclosure, the HP BladeSystem c3000 Enclosure, and all the server blades and networks contained within the enclosure.

The Virtual Connect Ethernet modules enable connection to all brands of data center Ethernet switches.

The Virtual Connect Ethernet modules can also be connected to other devices, such as printers, laptops, rack servers, and storage devices. To connect to devices other than switches, create a VC network for that device and only connect uplinks for that network to that device. If you connect uplinks from that network to other devices, one of the uplinks becomes standby due to the loop avoidance algorithm.

The Virtual Connect FC modules enable connection of the enclosure to Brocade, Cisco, McDATA, or QLogic data center Fibre Channel switches, but the modules do not appear as switches to the Fibre Channel fabric.

A basic Virtual Connect domain includes a single HP c-Class BladeSystem c7000 Enclosure for a total of 16 servers (or up to 32 servers if the double-dense option is enabled), or a single HP c-Class BladeSystem c3000 Enclosure for a total of eight servers (or up to 16 servers if the double-dense option is enabled). Within the domain, any server blade can access any LAN or SAN connected to a VC module, and a server blade can be used as a spare for any server blade within the same enclosure.

By stacking (cabling) the Ethernet modules within the domain and connecting the FC modules to the same set of FC SANs, every server blade in the domain can be configured to access any external network connection. With this configuration, the administrator can use Virtual Connect Manager to deploy and migrate a server blade profile to any server in the Virtual Connect domain without changing external LAN or SAN configurations.

Using multiple enclosures

Multiple enclosure support enables up to four c7000 enclosures to be managed within a single Virtual Connect domain for a total of 128 servers, if double-dense support is enabled. Multiple enclosure domains are not supported on c3000 enclosures. The VC-Enet modules use stacking cables between enclosures so that network traffic can be routed from any server Ethernet port to any uplink within the VC domain.

By stacking (cabling) the Ethernet modules within the domain, every server blade in the domain can be configured to access any external network connection. Fibre Channel modules within different enclosures are each connected directly to the same set of FC SANs. With this configuration, the administrator can use Virtual Connect Manager to deploy and migrate a server blade profile to any server in the Virtual Connect domain without changing external LAN or SAN configurations.

Using multiple c7000 enclosures, you can install up to 16 VC-Enet modules and up to 16 VC-FC modules in the same domain, with a maximum of 8 VC-Enet or 4 VC-FC modules per enclosure.

The management interfaces for all enclosure OAs and VC modules within the same VC domain must be on the same lightly loaded subnet. The OA IP addresses used must be configured to be static.

Command line overview

The HP Virtual Connect Manager Command Line Interface can be used as an alternative method for managing the Virtual Connect Manager. Using the CLI can be useful in the following scenarios:

- HP Management Applications (for example, Systems Insight Manager or Insight Control tools) can query the Virtual Connect Manager for information these tools need to present a complete management view of HP BladeSystem enclosures and devices. This interface is also used by the Management tools to execute provisioning and configuration tasks to devices within the enclosure.
- Users can develop tools that utilize Virtual Connect Manager functions for data collection and for executing provisioning and configuration tasks.

- When no browser is available or you prefer to use a command line interface, you can access management data and perform configuration tasks.

Command line syntax

CLI input is case-insensitive except when otherwise noted. The general CLI syntax format is as follows:

```
<subcommand> <managed element> <parameters> [<options>] [<properties>]
```

Item	Description
subcommand	Operation performed on a managed element
managed element	Management entity being operated on
parameters	Command extensions for a particular management operation
options	Attributes used to customize or control command execution behavior such as output format, quiet-mode, and others
properties	One or more name or value pairs that are accessories to the command operation, mainly for set and add operations

Example: `->add user mark password=asdf89g fullname="Mark Smith" enabled=true`

In the above example, `add` is the subcommand, `user` is the managed element, `mark` is a required parameter for the operation, `password` is a required property, and `fullname` and `enabled` are optional properties.

Depending on the specific command being executed, certain parameters or properties might be required. For example, when adding a new user, both a parameter representing the user name, as well as a password (in the form of a property) are required to be specified. All other user properties are optional at the time the user is added. In general, the properties are in the format `name=value`, and more than one property is separated by a space.

Parameters

Parameters are command extensions that provide extra information needed for the execution of a particular command. Whether or not a parameter is required depends on the specific command being executed. For example, the `show user` command has an optional parameter, which represents the user name if the user instance is being managed. If `show user` is entered, then a summary listing of all users is shown. However, if the optional parameter (`user name`) is provided, only a single user instance is displayed, for example, `show user paul`.

Some commands require that a parameter be specified, for example, the `add user` command. The required parameter is the user name (`add user jake`), and if the username is not provided, an error message displays indicating that a required parameter is missing.

Options

Options enable users to control certain behavior characteristics available during the command execution. Some examples of options include controlling output format and specifying a `quiet` mode for suppressing interactive prompts that would normally require input from the user.

Options are distinguished from other command line elements by using a hyphen (-) in front of the option. Option arguments are required or optional depending on the option being specified. For example, the –output option requires an argument, which is a list of one or more output format attributes. However, the -quiet option does not require any arguments to be specified.

The general format of a CLI option is as follows:

```
-<option>[=argument1>,<argument2>, . . .]
```

Example: `->show user suzi -output=script1`

In the example, `-output` is the option, and `script1` is an option argument.

Properties

Properties are specific configuration attributes of a managed element. Properties are commonly used during `set` operations or `add` operations where a managed element is being modified or created. In some limited circumstances, properties might also be used as a part of a `show` or other command.

IMPORTANT: If a property value contains embedded spaces, then the entire property value must be contained within single or double quotes. Likewise, if a double quote is part of a property value, it should be contained within single quotes, and if a single quote is part of a property value, it should be contained within double quotes.

Command batching

In previous versions of the CLI, the user had the following options to enable different CLI command invocations:

- Interactively input commands at the shell after logging in via SSH. This method works well for interactive users, but not necessarily for automation. Although users could write expect scripts for command processing, the solution is not optimal.
- Enter remote shell script commands, one-at-a-time, using a remote SSH client. This method enhances automation, but performance is lessened because each command requires logging in and logging out of the remote SSH server in the firmware. Because the authentication and command processing is performed over an encrypted channel, users experience a performance hit. If the user script is performing many operations in the client script, the time necessary to perform the tasks increases.

The updated version of the CLI supports a new enhancement that enables users to enter multiple CLI commands in a single command-line invocation. This capability is useful in situations where users prefer to batch several commands together and execute them in a particular sequence, within the context of the same user login SSH session. This method improves the overall performance of lengthy script processing.

Example 1: Sample commands with no command batching

```
add profile Profile1
add network Network1
add uplinkset UplinkSet1
```

Example 2: Sample commands using command batching

```
add profile Profile1;add network Network1;add uplinkset UplinkSet1
```

Supporting comments and blank lines in CLI scripts

Scripts are useful for batching many CLI commands. Administrators can create a single CLI script to configure an entire VC domain from scratch and use it on multiple enclosures.

The updated version of the CLI supports command scripts that contain blank lines and comments. In previous firmware versions, all commands that were provided as input to the CLI through scripts could only be valid commands. Supporting comments and blank lines enables users to maintain descriptive comments and notes in the configuration script more easily.

When using a Linux SSH client, simply redirect the script into SSH. If the SSH keys are not configured on the client and in the firmware, a password prompt appears. To allow script automation and better security, SSH public/private key-pairs can be generated and uploaded to the public key to the VC firmware.

```
>ssh Admin@192.168.0.120 < myscript.txt
```

When using a Windows-based SSH client, pass the file to the client using the `-m` option. If the SSH keys are not configured on the client and in the firmware, a password prompt appears. To allow script automation and better security, SSH public/private key-pairs can be generated and uploaded to the public key to the VC firmware.

```
>plink Admin@192.168.0.120 -m myscript.txt
```

The following sample script illustrates a CLI script that contains this type of formatting. Note that all comment lines must begin with "#".

```
#-------------------------------------------------------------------------
# This is my sample Virtual Connect Domain Configuration Script
# Revision 1.0.1.2
# February 15, 2008
#-------------------------------------------------------------------------

# Add Some Users
add user SomeNetworkUser password=pass1 privileges=network
add user SomeStorageUser password=pass2 privileges=storage
add user SomeDomainUser password=pass6 privileges=domain
add user SomeAdminUser password=pass3 privileges=*
add user DomainNetworkUser password=764dhh privileges=domain,network

# Add Some Profiles with Default VC-Enet and VC-FC Connections
add profile MyProfile
add profile AnotherProfile
add profile Profile45

# Add a few VC-Enet Networks
add network MyNetwork
add network Network2
```

```
# Add a few uplink ports to the networks
add uplinkport enc0:1:1 network=MyNetwork
add uplinkport enc0:1:2 network=Network2

# Create a Shared Uplink Port Set
add uplinkset SharedSet1

# Assign a profile to a device bay
assign profile MyProfile enc0:1

# Done!!!
```

Unassigning multiple profiles

In previous firmware releases, if the user needed to unassign multiple profiles from several device bays, the `unassign profile <profileName>` command could be used at the command line. When many profiles need to be unassigned, sending a command for each server profile to be unassigned can be tedious.

To simplify this scenario, the remove profile command has been extended to include unassigning multiple profiles from device bays with a single command.

The following example illustrates four server profiles being unassigned from device bays with a single CLI command. If an operation fails on one of the device bays, an ERROR message displays for that server/device bay, but the remaining operations continue.

```
->unassign profile *
SUCCESS: Profile1 unassigned from device bay enc0:1
SUCCESS: MyProfile2 unassigned from device bay enc0:2
SUCCESS: GreenProfile unassigned from device bay enc0:3
SUCCESS: RedProfile unassigned from device bay enc0:4
```

CLI command execution modes

The Virtual Connect Manager CLI provides two different methods for executing commands: interactive shell mode and non-interactive mode.

Interactive Shell Mode

This mode is used to invoke CLI command operations using the dedicated management shell. The shell is provided after the user logs in with valid credentials, and only accepts known VCM CLI commands as input. Users can quit the shell by using the `exit` command. An example of logging into the interactive management shell is provided below. In the example, the primary VCM is located at IP address 192.168.0.120.

```
>ssh 192.168.0.120
```

```
login as: michael
password: ***********

------------------------------------------------------------------------
HP Virtual Connect Management CLI v3.00
(C) Copyright 2006-2007 Hewlett-Packard Development Company, L.P.
All Rights Reserved
------------------------------------------------------------------------

GETTING STARTED:

help           : displays a list of available subcommands
exit           : quits the command shell
<subcommand> ? : displays a list of managed elements for a subcommand
<subcommand> <managed element> ? : displays detailed help for a command

->
```

Non-Interactive Mode

In some cases, users might want to write automated scripts that execute a single command at a time. These scripts can be used to batch several commands in a single script file from the SSH client. An example of how to use the non-interactive mode for CLI command execution is provided below. In the example, the primary VCM is located at IP address 192.168.0.120.

IMPORTANT: To suppress prompting for a password during login, you must first setup the SSH encryption keys using the VCM Web GUI, and configure your SSH client properly with the keys. For additional information on configuring the SSH keys, see the *HP Virtual Connect for c-Class BladeSystem User Guide*.

```
->ssh Administrator@192.160.0.120 show enclosure
<command output displayed to console>
```

Remote access to the Virtual Connect Manager

The Virtual Connect Manager CLI can be accessed remotely through any SSH session:

1. Start an SSH session to the Virtual Connect Manager using any SSH client application.
2. When prompted, type the assigned IP address or DNS name of the Virtual Connect Manager, and then press **Enter.**
3. Type a valid user name, and then press **Enter.**
4. Type a valid password, and then press **Enter.** The CLI command prompt displays.
5. Enter commands for the Virtual Connect Manager.
6. To terminate the remote access SSH session, close the communication software or enter `exit` at the CLI command prompt.

Command output filtering

The CLI provides output filtering capabilities that enable users to display only properties of interest. This feature is useful for filtering large amounts of output data for specific information. One or more properties can be specified in the output filtering rules.

The examples below illustrate some common usage scenarios for output filtering.

Example 1: Displaying all enabled users

```
->show user enabled=true
```

Example 2: Displaying on VC Ethernet Interconnect Modules

```
->show interconnect type=VC-ENET
```

Example 3: Displaying all external uplink that have a link established

```
->show uplinkport status=linked
```

Example 4: Displaying all uplink ports with connector type of RJ-45 and speed configured to Auto

```
->show uplinkport type=RJ45 Speed=Auto
```

Example 5: Displaying all servers currently powered on

```
->show server power=On
```

Command line

Subcommands

Command	Description
add	Add a new object to the domain or to another object
assign	Assign a server profile to a device bay
delete	Delete the domain configuration
exit	Exit the Virtual Connect Manager command-line shell
help	Display context-sensitive help for a command or object
import	Import an enclosure into the domain
load	Transfer a file from a remote location to the domain
poweroff	Power off one or more servers
poweron	Power on one or more servers
reboot	Reboot one or more servers
remove	Remove or delete an existing object (for example, users or profiles)
reset	Perform a reset operation on an object (for example, vcm)
save	Transfer a file from the domain to a remote location
set	Modify one or more configuration properties of an object
show	Display properties or information about an object
test	Test the configuration of an object (for example, log-target)
unassign	Unassign a server profile from a device bay

Managed elements

Managed element	Description
all (on page 15)	Display all VC domain-managed elements
devicebay (on page 15)	Display enclosure device bay information
domain (on page 16)	Manage general Virtual Connect domain settings and information
enclosure (on page 18)	Manage general enclosure settings and information
enet-connection (on page 20)	Manage Ethernet network connections
enet-vlan (on page 23)	Manage Ethernet VLAN connections
external-manager (on page 24)	Manage external manager settings and information
fabric (on page 26)	Manage Fibre Channel SAN fabrics
fc-connection (on page 29)	Manage Fibre Channel SAN fabric connections

Managed element	Description
`firmware` (on page 31)	Manage interconnect module firmware
`igmp` (on page 32)	Manage Ethernet IGMP Snooping settings
`interconnect` (on page 32)	Manage I/O interconnect modules
`ldap` (on page 33)	Manage LDAP configuration settings
`ldap-certificate` (on page 35)	Manage LDAP certificate information
`ldap-group` (on page 36)	Manage LDAP group configuration settings
`log-target` (on page 37)	Manage remote log destination settings
`mac-cache` (on page 40)	Manage Ethernet MAC cache failover settings
`network` (on page 40)	Manage Virtual Connect Ethernet networks
`port-monitor` (on page 44)	Monitor port monitor configurations
`profile` (on page 46)	Manage Virtual Connect server profiles
server (on page 49)	Manage physical HP BladeSystem servers
`serverid` (on page 52)	Manage virtual server ID configuration settings
`server-port` (on page 53)	Display all physical server ports
`server-port-map` (on page 54)	Manage shared server downlink port mapping configuration
`snmp` (on page 56)	Modify SNMP configurations
`snmp-trap` (on page 57)	Modify SNMP-trap configurations
`ssh` (on page 60)	Display SSL configuration and information
`ssl-certificate` (on page 61)	Manage SSL certificate information
`ssl-csr` (on page 62)	Manage an SSL certificate signing request
`ssl` (on page 61)	Manage weak SSL encryption
`stackinglink` (on page 63)	Display stacking link information and status
`statistics` (on page 63)	Display or reset statistics on a designated interconnect module port
`status` (on page 64)	Display overall Virtual Connect domain status information
`supportinfo` (on page 64)	Manage Virtual Connect support information
`systemlog` (on page 64)	Display Virtual Connect Manager system event log
`uplinkport` (on page 65)	Manage interconnect module uplink ports
`uplinkset` (on page 68)	Manage shared uplink port sets
`user` (on page 69)	Manage local Virtual Connect user configurations
`user-security` (on page 71)	Manage user security settings
`vcm` (on page 72)	Manage the Virtual Connect domain manager
`version` (on page 73)	Display CLI version information

The following sections provide detailed information on how the subcommands are used with each managed element.

To display command help, enter a command followed by `?` or `-help`. For additional information on the `help` subcommand, see "Help subsystem (on page 73)."

all

Manage all Virtual Connect domain elements.

Supported actions: `help, show`

Item	Description
`show all`	Display all Virtual Connect domain configuration objects. This command is typically useful for displaying a snapshot of the entire domain configuration with a single command.
Syntax	`show all [*]`
Examples	
	`->show all` Displays all configuration objects (summary view)
	`->show all *` Displays all configuration objects (detailed view)

devicebay

Manage general enclosure device bay settings and information.

Supported actions: `help, show`

Item	Description
`show devicebay`	Display device bays of all enclosures that exist in the Virtual Connect domain.
Syntax	`show devicebay [<DeviceBayID>|*]`
Parameter	
`DeviceBayID (Optional)`	The reference ID of a device bay in the domain The format of the device bay ID is `<EnclosureID:DeviceBay>`. Example: "enc0:1" indicates device bay 1 of the local enclosure being managed. If * is specified, then all enclosures appear with detailed output format. If EnclosureID is not specified, the default enclosure is the local enclosure where the Virtual Connect manager and domain exist. If a multi-blade server is present then use the DeviceBayID of the monarch bay. This is the ID value shown by show devicebay.
Examples	
	`->show devicebay` Displays a summary listing of all device bays
	`->show devicebay *` Displays detailed information for all device bays
	`->show devicebay enc0:2` Displays detailed information for a specific device bay of a specific enclosure
	`->show devicebay enc1:4` Displays detailed information for a specific device bay 4 of a remote enclosure
	`->show devicebay enc0:5`

Item	Description
	Displays detailed information for a multi-blade server in device bays 5-8 of the primary enclosure.

domain

Manage general Virtual Connect domain settings and information.

Supported actions: `delete, help, set, show`

Item	Description
`delete domain`	Delete the existing Virtual Connect domain configuration. Deleting the domain removes the entire Virtual Connect domain configuration and resets it to the original defaults. After the domain has been deleted, you are logged out and the Virtual Connect Manager resets.
Syntax	`delete domain [-quiet]`
Option	
`quiet`	Suppresses user confirmation prompts. This option is useful when scripting delete domain operations.
Examples	
	`->delete domain` Deletes the Virtual Connect domain configuration and prompts for user confirmation
	`->delete domain -quiet` Deletes the Virtual Connect domain quietly without prompting for user confirmation (primarily used in automated scripting scenarios)

Item	Description
`set domain`	Modify general Virtual Connect domain configuration properties, such as the domain name, domain IP address, and MAC and WWN address pool settings.
Syntax	`set domain [Name=<NewName>] [DomainIp=<Enabled|Disabled>] [IpAddress=<IPAddress>] [SubnetMask=<mask>] [Gateway=<Gateway>] [MacType=<VC-Defined|Factory-Default|User-Defined>] [MacPool=<1-64>] [MacStart=<MAC address>] [MacEnd=<MAC address>] [WwnType=<VC-Defined | Factory-Default | User-Defined>] [WwnPool=<1-64>] [WwnStart=<WWN Address>] [WwnEnd=<WWN Address>] [SingleDense=true|false]`
Properties	
`Name (optional)`	The new name of the domain. Valid characters include alphanumeric, "_", and ".". The maximum length of the name is `31` characters.
`DomainIP (optional)`	Enables or disables the Virtual Connect domain IP address. If enabled, then a valid IP address subnet mask must be configured. If disabled, then DHCP is used to obtain a valid IP address. Enabling domain IP address configuration or changing the domain IP address can cause a temporary loss of connectivity to the Virtual Connect Manager. Use caution when changing these settings. Valid values include "Enabled" and "Disabled".
`IpAddress (optional)`	A valid IP address to use for the domain IP address configuration. The IP address must be in the format xxx.xxx.xxx.xxx, where x is a number between 0

Item	Description
	and 9. Example: 192.168.0.10
SubnetMask (Required if IP address specified)	A valid subnet mask for the domain IP address configuration. The subnet mask must be in the format xxx.xxx.xxx.xxx, where x is a number between 0 and 9. Example: 255.255.255.0
Gateway (Required if IP address specified)	A valid gateway address for the domain IP address configuration. The gateway address must be in the format xxx.xxx.xxx.xxx, where x is a number between 0 and 9. Example: 192.168.0.1
MacType (optional)	The type of MAC address source to use for assignment. Valid values include "VC-Defined", "Factory-Default", and "User-Defined".
MacPool (optional)	The pre-defined MAC pool to use for address assignment. Valid values include integers 1-64. This property is only valid if the MacType is set to "VC-Defined". If not specified, the default pool ID is 1.
MacStart (Required if MacType is User-Defined)	The starting MAC address in a custom user-defined range. This property is only valid if the MacType is set to "User-Defined".
MacEnd (Required if MacType is User-Defined)	The ending MAC address in a custom user-defined range. This property is only valid if the MacType is set to "User-Defined".
WwnType(optional)	The type of WWN address source to use for assignment. Valid values include "VC-Defined", "User-Defined", and "Factory-Default".
WwnPool(optional)	The pre-defined WWN pool to use for address assignment. Valid values include integers 1-64. This property is only valid if the WwnType is set to "VC-Defined". If not specified, the default pool ID is 1.
WwnStart (Required if WwnType is User-Defined)	The starting WWN address in a custom user-defined range. This property is only valid if the WwnType is set to "User-Defined".
WwnEnd (Required if WwnType is User-Defined)	The ending WWN address in a custom user-defined range. This property is only valid if the WwnType is set to "User-Defined".
SingleDense (optional)	If the imported domain supports double-dense server blades, this property enables the device bay display format to support the display for single-dense servers along with the double-dense servers. In a double-dense supported configuration, the default for this property is false, which disables the display of single-dense servers.
Examples	
	`->set domain Name=MyNewDomainName` Changes the name of the Virtual Connect domain
	`->set domain DomainIp=Enabled` Enables the domain IP address
	`->set domain DomainIp=Enabled IpAddress=192.168.0.120 SubnetMask=255.255.255.0 Gateway=192.168.0.1` Configures the domain IP address and enables it
	`->set domain DomainIp=Disabled` Disables the domain IP address and uses DHCP instead
	`->set domain MacType=VC-Defined MacPool=10` Sets the MAC address source to VC-Defined with a pre-defined range
	`->set domain MacType=Factory-Default` Sets the MAC address source to use factory default MAC addresses

Item	Description
	`->set domain MacType=User-Defined MacStart=00-17-A4-77-00-00 MacEnd=00-17-A4-77-00-FF` Sets the MAC address source to a custom, user-defined address range
	`->set domain WwnType=VC-Defined WwnPool=5` Sets the WWN address source to VC-Defined with a pre-defined range
	`->set domain WwnType=Factory-Default` Sets the WWN address source to use factory default WWN addresses
	`->set domain WwnType=User-Defined WwnStart=50:06:0B:00:00:C2:62:00 WwnEnd=50:06:0B:00:00:C2:62:FF` Sets the WWN address source to a custom, user-defined address range
	`->set domain SingleDense=true` Sets the display option to support single-dense servers in a double-dense supported configuration

Item	Description
`show domain`	Display general Virtual Connect domain information, including the Virtual Connect domain name, the VCM domain IP address settings, and MAC/WWN address settings for the domain.
Syntax	`show domain [addressPool]`
Parameter	
`addressPool (Optional)`	Displays all the VC-defined address pool range available for use
Examples	
	`->show domain` Displays domain information
	`->show domain addressPool` Displays the VC-defined address pools for the domain

enclosure

Manage general enclosure settings and information.

Supported actions: `help, import, remove, show`

Item	Description
`import enclosure`	Import local and remote enclosures into the Virtual Connect domain. Virtual Connect supports up to four c7000 enclosures in a single domain.
Syntax	`import enclosure [IpAddress] [UserName=<username>] [Password=<password>] [DoubleDense=<True|False>]` For enclosures that are not imported, the password field is optional on the command line. If not specified on the command line, the system interactively prompts the user for the same password.
Parameter	
`IpAddress (Optional)`	The IP address or DNS name of the remote enclosure to be imported. If the IP address is not given, then the local enclosure is assumed.
Properties	

Item	Description
`UserName (Required for enclosures that are not imported)`	A valid user name of the Onboard Administrator user for the enclosure to be imported.
`Password (Required)`	A valid OA user password for importing the enclosure. If no password is given at the command line, the system interactively prompts the user for a password during the import operation.
`DoubleDense (Optional)`	If the enclosure being imported supports double-dense servers, then this property enables the device bay display format to support a display for double-dense servers. The default behavior is display for single-dense servers in the enclosure.
Examples	
	`->import enclosure UserName=Administrator Password=fgg7h*1` Imports the local enclosure into the domain
	`->import enclosure UserName=Administrator Password=fgg7h*1 DoubleDense=true` Imports the local enclosure with a double-dense device bay display format
	`-> import enclosure 192.168.0.120 UserName=MyOaUser Password=dgfsfdsjd` Imports a remote enclosure into the domain
	`-> import enclosure` Imports the local enclosure that is already discovered
	`-> import enclosure 192.168.0.120` Imports a remote enclosure that is already discovered

Item	Description
`remove enclosure`	Remove a remote enclosure that has been imported into the domain. The local enclosure cannot be removed from the domain using the `remove enclosure` command.
Syntax	`remove enclosure <EnclosureID | *>`
Parameter	
`EnclosureID (required)`	The enclosure ID of the remote enclosure to be removed from the domain, where "*" removes all the remote enclosures that exist in the domain. The enclosure IDs can be identified for a particular enclosure by using the `show enclosure` command. The local enclosure cannot be removed from the domain with this command.
Examples	
	`->remove enclosure encl` Removes a remote enclosure
	`->remove enclosure *` Removes all remote enclosures from the domain

Item	Description
`show enclosure`	Display all enclosures in the domain.
Syntax	`show enclosure [<EnclosureID>|*]`
Parameter	

Item	Description
`EnclosureID (optional)`	The ID of an enclosure in the domain. If specified, then only details for the specified enclosure appear.
Examples	
	`->show enclosure` Displays a summary listing of all enclosures
	`->show enclosure *` Displays detailed information for all enclosures
	`->show enclosure enc0` Displays detailed information for a specific enclosure

enet-connection

Manage Ethernet network connections.

Supported actions: `add, help, remove, set, show`

Item	Description
`add enet-connection`	Add a new Ethernet network connection to an existing server profile. The maximum number of Ethernet connections that can be added to a server profile is 128.
Syntax	`add enet-connection <ProfileName> [Network=<NetworkName>] [PXE=<enabled|disabled|UseBios>] [AddressType=<Factory-Default|User-Defined>] [EthernetMAC=<MAC Address> iScsiMAC=<MAC Address>] [SpeedType=<Auto|Preferred|Custom>] [Speed=<speed>]`
Parameter	
`ProfileName (required)`	The name of an existing profile to which the new connection is added.
Properties	
`Network (optional)`	The name of an existing network to associate with the connection. If the network name is not specified, or is set to "unassigned", then the network remains unassigned and can be assigned later.
`PXE (optional)`	Enables or disables PXE on the network connection. Valid values are "enabled", "disabled", and "UseBios". If this value is not specified, the default is "UseBios". Only one connection can have PXE enabled per profile.
`AddressType (optional)`	The source of MAC address assignments to be used during the creation of the new connection. If not specified, the default is the domain default. If "User-Defined" is specified, then both an Ethernet MAC Address and iSCSI MAC Address must also be specified. Valid values include "Factory-Default" and "User-Defined".
`EthernetMAC (required if AddressType is User-Defined)`	The user-defined Ethernet MAC address to use for the connection. This property is required if the AddressType specified is "User-Defined".
`iScsiMAC (required if AddressType is User-Defined)`	The user-defined iSCSI MAC address to use for the connection. This property is required if the AddressType specified is "User-Defined".
`SpeedType (optional)`	The requested operational speed for the server port. Valid values include "Auto", "Preferred", and "Custom". The default value is

Item	Description
	"Preferred". If the speed type is "Auto", the maximum port speed is determined by the maximum configured speed for the network. If the speed type is "Preferred", the speed of the network is the same as the preferred speed of the network to which the connection is associated. If no preferred speed is configured for a network, it defaults to "Auto". If the speed type is "Custom", the user can configure any speed from 100Mb to MAX configured speed for the network in 100Mb increments.
`(Speed (required if the SpeedType is Custom)`	The user-defined speed for the server port. Valid values include 100Mb to MAX configured speed for the network in 100Mb increments.
Examples	
	`->add enet-connection MyNewProfile Network=SomeNetwork` Adds a new Ethernet network connection to a profile
	`->add enet-connection MyNewProfile Network=SomeNetwork2 PXE=enabled` Adds a new Ethernet network connection and enables PXE
	`->add enet-connection MyNewProfile` Adds a new Ethernet network connection and leaves the network unassigned
	`->add enet-connection MyNewProfile AddressType=Factory-Default` Adds a new Ethernet network connection and uses factory default addresses
	`->add enet-connection MyNewProfile AddressType=User-Defined EthernetMAC=00-17-A4-77-00-00 iScsiMAC=00-17-A4-77-00-01` Adds a new Ethernet network connection and provides user-defined MAC addresses
	`->add enet-connection MyProfile Network=MyNetwork SpeedType=Preferred` Adds a new Ethernet network connection and sets the speed to "Preferred"
	`->add enet-connection MyProfile Network=MyNetwork SpeedType=Custom Speed=2000` Adds a new Ethernet network connection and sets the speed to 2Gb

Item	Description
`remove enet-connection`	Remove the last Ethernet network connection from an existing server profile.
Syntax	`remove enet-connection <ProfileName>`
Parameter	
`ProfileName (required)`	The name of the profile from which to remove the Ethernet connection.
Example	

Item	Description
	`->remove enet-connection MyProfile` Removes an Ethernet network connection from a profile.

Item	Description
`set enet-connection`	Modify an Ethernet connection of a server profile.
Syntax	`set enet-connection <ProfileName> <Port> [Network=<NetworkName>] [PXE=<enabled|disabled|UseBios>] [SpeedType=<Auto|Preferred|Custom>] [Speed=<speed>]`
Parameters	
`ProfileName (required)`	The name of the server profile that contains the connection to modify
`Port (required)`	The port number of the connection being modified
Properties	
`Network (optional)`	The name of the Ethernet network to associate with the connection. Applies to Ethernet network connections only. A blank string makes the Ethernet connection unassigned.
`PXE (optional)`	Enables or disables PXE on a connection. Valid values are "enabled", "disabled", and "UseBios". Applies to Ethernet network connections only. PXE can be enabled on one connection per profile.
`SpeedType (optional)`	The requested operational speed for the server port. Valid values include "Auto", "Preferred", and "Custom". The default value is "Preferred". If the speed type is "Auto", the maximum port speed is determined by the maximum configured speed for the network. If the speed type is "Preferred", the speed of the network is the same as the preferred speed of the network to which the connection is associated. If no preferred speed is configured for a network, it defaults to "Auto". If the speed type is "Custom", the user can configure any speed from 100Mb to MAX configured speed for the network in 100Mb increments.
`Speed (required if the SpeedType is Custom)`	The user-defined speed for the server port. Valid values include 100Mb to MAX configured speed for the network in 100Mb increments.
Examples	
	`->set enet-connection MyProfile 2 Network=NewNetworkName` Changes the associated network of an Ethernet connection
	`->set enet-connection RedProfile 1 Network=""` Sets a network connection to "Unassigned"
	`->set enet-connection GreenProfile 3 PXE=disabled` Disables PXE on an Ethernet connection
	`->set enet-connection MyProfile 1 SpeedType=Preferred` Modifies the Ethernet network connection to set the speed to "Preferred"

Item	Description
	`->set enet-connection MyProfile 1 SpeedType=Custom Speed=2000` Modifies the Ethernet network connection to set the speed to 2Gb

Item	Description
`show enet-connection`	Display the ethernet connections associated with the server profiles.
Syntax	`show enet-connection [<ConnectionID>]`
Parameter	
`ConnectionID (optional)`	The ID of an existing Ethernet connection. The ID format is `<ProfileName:Port>`. `<ProfileName:*>` can be used to display all profile Ethernet connections. "*" displays all connections existing in the domain.
Examples	
	`->show enet-connection` Displays all Ethernet connections existing in the domain
	`->show enet-connection Profile1:*` Displays Ethernet connections of a profile Profile1
	`->show enet-connection Profile1:1` Displays a specific Ethernet connection of profile Profile1

enet-vlan

Manage Ethernet VLAN configuration settings.

Supported actions: `help, set, show`

Item	Description
`set enet-vlan`	Modify general Ethernet VLAN configuration settings.
Syntax	`set enet-vlan [VLanTagControl=<Tunnel|Map>] [SharedServerVLanId=<true|false>] [PrefSpeedType=<Auto|Custom>] [PrefSpeed=<speed>] [MaxSpeedType=<Unrestricted|Custom>] [MaxSpeed=<speed>]`
Properties	
`VLanTagControl (optional)`	Determines how Ethernet packet VLAN tags are handled by the domain. Valid values include "Tunnel" and "Map". The "tunnel" option enables VLAN tagging support only on networks with dedicated uplinks. Also, Ethernet ports connected to networks using shared uplink sets can transmit and receive untagged frames only. The "Map" option enables the user to add more than one network to a single Ethernet port for the server profiles, and also enables the user to specify VLAN mapping between server tags and VC networks. Also, Ethernet networks with dedicated uplinks can transmit and receive untagged frames only.
`SharedServerVLanId (optional)`	Enables or disables the option to force server ports connected to multiple VC Ethernet networks to use the same VLAN mappings as those used by corresponding shared uplink sets. Valid values include "true" and "false".

Item	Description
	Setting the value to "true" restricts the server network connections to be selected from a single shared uplink, and the VLAN ID cannot be modified. Setting the value to "false" enables the user to select any VC Ethernet network for the server Ethernet connections, and VLAN ID mappings can be modified to ensure uniqueness. SharedServerVLanId can be "true" only if VLanTagControl is set to "Map".
`PrefSpeedType (optional)`	The default connection speed for any Ethernet connection using multiple networks. Valid values include "Auto" and "Custom". "Custom" allows the user to configure the preferred speed. The default value is "Auto".
`PrefSpeed (required if PrefSpeedType is Custom)`	The default connection speed for any Ethernet connection using multiple networks. Valid values range from 100Mb to 10Gb in 100Mb increments.
`MaxSpeedType (optional)`	Maximum connection speed for any Ethernet connection using multiple networks. Valid values include "UnRestricted" and "Custom". "Custom" allows the user to configure the preferred speed. The default value is "Unrestricted".
`MaxSpeed (required if MaxpeedType is Custom)`	The maximum connection speed for any Ethernet connection using multiple networks. Valid values range from: 100Mb to 10Gb in 100Mb increments.
Examples	
	`->set enet-vlan VLanTagControl=Map SharedServerVLanId=true` Sets the VLanTagControl to Map and SharedServerVLanId to Enabled
	`->set enet-vlan PrefSpeedType=Custom PrefSpeed=500 MaxSpeedType=Custom MaxSpeed=2500` Sets the preferred connection speed for all connections using multiple networks to 500Mb, and the maximum connection speed to 2.5Gb

Item	Description
`show enet-vlan`	Display general Ethernet VLAN configuration settings.
Syntax	`show enet-vlan`
Example	
	`->show enet-vlan` Displays Ethernet VLAN configuration settings

external-manager

Manage external manager settings and information.

Supported actions: `remove, help, set, show`

Item	Description
`remove external-manager`	Remove an existing external manager (VCEM) and regain local management profile control of the domain. When releasing the profile control, it is mandatory to specify values for each MacType, WwnType, and ServerIdType.
Syntax	`remove external-manager [-quiet] [UserName=<username>] [MacType=<Factory-Default| User-Defined>] [MacStart=<MAC`

Item	Description
	address>] [MacEnd=<MAC address>] [WwnType=<Factory-Default|User-Defined>] [WwnStart=<WWN address>] [WwnEnd=<WWN address>] [ServerIdType=<Factory-Default|User-Defined>] [ServerIdStart=<ServerId address>] [ServerIdEnd=<ServerId address>]
Option	
quiet	This option suppresses user confirmation prompts and is useful when scripting operations.
Properties	
UserName (optional)	A valid external manager user name. The user name can be identified using the show external-manager command.
MacType (optional)	The type of MAC address source to use for assignment. Valid values include "Factory-Default" and "User-Defined".
MacStart (required if the MacType is User-Defined)	The starting MAC address in a custom user-defined range. This property is only valid if the MacType is set to "User-Defined".
MacEnd (required if the MacType is User-Defined)	The ending MAC address in a custom user-defined range. This property is only valid if the MacType is set to "User-Defined".
WwnType (optional)	The type of WWN address source to use for assignment. Valid values include "Factory-Default" and "User-Defined".
WwnStart (required if the WwnType is User-Defined)	The starting WWN address in a custom user-defined range
WwnEnd (required if the WwnType is User-Defined)	The ending WWN address in a custom user-defined range
ServerIdType (optional)	The type of the virtual serial number source. When server profiles are created, the virtual serial numbers and UUID values are allocated from the specified pool source. Valid values include "Factory-Default" and "User-Defined".
ServerIdStart (required if Type is User-Defined)	The starting serial number in a user-defined range. This property is only valid for user-defined serial number types.
ServerIdEnd (required if Type is User-Defined)	The ending serial number in a user-defined range. This property is only valid for user-defined serial number types.
Examples	
	->remove external-manager UserName=A17005068 Removes only the external management control of the VC Manager
	->remove external-manager macType=Factory-Default wwnType=Factory-Default serverIdType=Factory-Default Releases only the profile control
	->remove external-manager username=A1010345 macType=Factory-Default wwnType=Factory-Default serverIdType=Factory-Default Removes the external manager and releases the profile control
	->remove external-manager username=A19216811 mactype=User-Defined MacStart=00-17-A4-77-00-00 MacEnd=00-17-A4-77-03-FF wwnType=User-Defined WwnStart=50:06:0B:00:00:C2:62:00 WwnEnd=50:06:0B:00:00:C2:65:FF serverIdType=User-Defined serverIdStart=VCX0000000 serverIdEnd=VCX00000ZZ

Item	Description
	Removes the external manager and releases the profile control

Item	Description
`set external-manager`	Enable or disable an existing external manager's control of the Virtual Connect domain.
Syntax	`set external-manager [-quiet] UserName=<username> Enabled=<true|false>`
Option	
`quiet`	This option suppresses user confirmation prompts and is useful when scripting operations.
Properties	
`UserName (required)`	A valid external manager user name. The user name can be identified using the `show external-manager` command.
`Enabled (required)`	Enables or disables the external manager. Valid values include "true" and "false".
Examples	
	`->set external-manager UserName=A17005068 Enabled=false` Disables the external manager
	`->set external-manager UserName=A17005068 Enabled=true` Enables the external manager

Item	Description
`show external-manager`	Display the information of an existing external manager.
Syntax	`show external-manager`
Example	
	`->show external-manager` Displays the information of an existing external manager

fabric

Manage Fibre Channel SAN fabrics.

Supported actions: `add, help, remove, set, show`

Item	Description
`add fabric`	Add a new VC Fibre Channel SAN Fabric to the domain.
Syntax	`add fabric <Name> Bay=<BayNum> Ports=<PortList> [Speed=<Auto|2Gb|4Gb|8Gb>] [LinkDist=<Auto|Manual>]`
Parameter	
`Name (required)`	A unique name for the new VC FC Fabric to be added to the domain
Properties	
`Bay (required)`	The specific interconnect bay number with which the fabric will be associated
`Ports (required)`	A list of one or more logical FC ports to be added to the fabric. Each port is

Item	Description
	specified in the format "<port1>,<port2>,...", where port is the interconnect module port number to be added to the fabric (affects all modules within a bay group). Example: "1, 2, 3, 4". For HP VC FlexFabric 10Gb/24-Port Modules, port numbers 1, 2, 3, and 4 correspond to ports X1, X2, X3, and X4, respectively.
`Speed (optional)`	The port speed for the uplink ports in the fabric. Valid values include "Auto", "2Gb", "4Gb', and "8Gb". The default port speed is "Auto". Speed restrictions: • For the HP 4Gb VC-FC Module and HP Virtual Connect 4Gb FC Module, valid speed values include "Auto", "2Gb", and "4Gb". • For the HP VC 8Gb 24-Port FC Module, HP VC 8Gb 20-Port FC Module, and HP VC FlexFabric 10Gb/24-Port Module, valid speed values include "Auto", "2Gb", "4Gb", and "8Gb".
`LinkDist (optional)`	Specifies the login re-distribution scheme to use for load balancing. Valid values include "Auto" and "Manual". The default login re-distribution is "Manual". The HP 4Gb VC-FC Module, HP Virtual Connect 4Gb FC Module, HP VC 8Gb 20-Port FC Module and HP VC 8Gb 24-Port Module support only manual login redistribution. The HP VC FlexFabric 10Gb/24-Port Module supports both auto and manual login redistribution.
Examples	
	`->add fabric MyFabric1 Bay=3 Ports=1,2` Adds a new fabric, using default values
	`->add fabric MyFabric2 Bay=3 Ports=1 Speed=2Gb` Adds a new fabric with speed set to 2Gb
	`->add fabric MyFabric3 Bay=3 Ports=1,2,3,4 LinkDist=Auto` Adds a new fabric with automatic login re-distribution
	`->add fabric MyFabric4 Bay=3 Ports=1,2` Adds a new fabric with two logical ports

Item	Description
`remove fabric`	Remove an existing VC FC SAN fabric from the domain.
Syntax	`remove fabric <Name|*>`
Parameter	
`Name (required)`	The name of a specific fabric, or "*" to remove all existing fabrics.
Examples	
	`->remove fabric VFabric_1` Removes VC FC SAN fabric VFabric_1
	`->remove fabric *` Removes all VC FC fabrics from the domain

Item	Description
`set fabric`	Modify properties of an existing FC SAN fabric. Can also be used to force load balancing of a fabric if login re-distribution is configured.
Syntax	`set fabric <Name> [-LoadBalance] [Name=<NewName>] [Ports=<PortList>] [Speed=<Auto|2Gb|4Gb|8Gb>] [LinkDist=<Auto|Manual>]`

Item	Description
Parameter	
`Name (required)`	A unique name for the fabric
Option	
`LoadBalance`	Performs load balancing on a fabric configured for manual login re-distribution
Properties	
`Name (optional)`	The new name of the fabric
`Speed (optional)`	The port speed for the uplink ports in the fabric Valid values include “Auto”, “2Gb”, "4Gb", and “8Gb”. The default port speed is “Auto”. Speed restrictions: • For the HP 4Gb VC-FC Module and HP Virtual Connect 4Gb FC Module, valid speed values include "Auto", "2Gb", and "4Gb". • For the HP VC 8Gb 24-Port FC Module, HP VC 8Gb 20-Port FC Module, and HP VC FlexFabric 10Gb/24-Port Module valid speed values include "Auto","2Gb","4Gb", and "8Gb".
`LinkDist (optional)`	Specifies the login re-distribution scheme for load balancing. Valid values include "Auto" and "Manual". The default login re-distribution is "Manual". The HP 4Gb VC-FC Module, HP Virtual Connect 4Gb FC Module, HP VC 8Gb 20-Port FC Module, and HP VC 8Gb 24-Port FC Module support only Manual login re-distribution. The HP VC FlexFabric 10Gb/24-Port Module supports both Auto and Manual login re-distribution schemes.
`Ports (optional)`	A list of one or more logical FC ports to be added to the fabric. Each port is specified in the format "<port1>,<port2>,...", where port is the interconnect module port to be modified in the fabric (affects all modules within a bay group). For HP VC FlexFabric 10Gb/24-Port Modules, port numbers 1, 2, 3, and 4 correspond to ports X1, X2, X3, and X4, respectively.
Examples	
	`->set fabric MyFabric1 Name=MyNewName1` Changes the name of an existing fabric
	`->set fabric MyFabric2 Speed=2Gb LinkDist=Auto` Modifies the port speed and login re-distribution
	`->set fabric MyFabric3 Ports=1,2,3,4` Modifies the fabric ports contained in the fabric
	`->set fabric MyFabric5 -loadBalance` Performs load balancing on a fabric with manual login re-distribution

Item	Description
`show fabric`	Display all FC SAN fabric information.
Syntax	`show fabric [<FabricName> | *]`
Parameter	
`Name (optional)`	Name of an existing FC SAN fabric. “*” displays a detailed output of all the fabrics in the VC domain. If not specified, a summary output of all fabrics appears.
Examples	
	`->show fabric` Displays a summary listing of all FC SAN fabrics
	`->show fabric *`

Item	Description
	Displays detailed information for all FC SAN fabrics
	`->show fabric SAN_5` Displays detailed information for a specific FC SAN fabric

fc-connection

Manage Fibre Channel SAN connections.

Supported actions: `add, help, remove, set, show`

Item	Description
`add fc-connection`	Add a new FC SAN connection to an existing server profile.
Syntax	`add fc-connection <ProfileName> [Fabric=<FabricName>] [Speed=<Auto|1Gb|2Gb|4Gb|8Gb|Disabled>] [AddressType=<Factory-Default|User-Defined>] [PortWWN=<WWN address>] [NodeWWN=<WWN address>]`
Parameter	
`ProfileName (required)`	The name of an existing profile to which the new connection is added
Properties	
`Fabric (optional)`	The name of an existing fabric to associate with the connection. If the fabric name is not specified, then the connection is marked as “Unassigned” but associated with a specific bay.
`Speed (optional)`	The port speed of the connection port. Valid values include "Auto", "1Gb", "2Gb", "4Gb", "8Gb", and "Disabled". If not specified, then the default port speed is set to "Auto". Speed restrictions: For the HP 4Gb VC-FC Module and HP Virtual Connect 4Gb FC Module, supported speed values include "Auto","1Gb","2Gb", and "4Gb", and "Disabled". If the value is set to 8Gb, the speed is auto-negotiated by Virtual Connect.
`AddressType (optional)`	The source of WWN address assignments to be used during the creation of the new connection. If not specified, the default is the domain default. If "UserDefined" is specified, then both a Port WWN and Node WWN must also be specified. Valid values include "Factory-Default" and "User-Defined".
`PortWWN (required if AddressType is User-Defined)`	The user-defined Port WWN address to use for the connection. This property is required if the AddressType specified is "User-Defined". The PortWWN must be an unused WWN address.
`NodeWWN (required if AddressType is User-Defined)`	The user-defined Node WWN address to use for the connection. This property is required if the AddressType specified is "User-Defined". The NodeWWN must be an unused WWN address.
Examples	
	`->add fc-connection MyNewProfile Fabric=SAN_5` Adds a new FC SAN fabric connection to a profile
	`->add fc-connection MyNewProfile Fabric=SomeFabric Speed=4Gb` Adds a new FC SAN connection and configures the port speed

Item	Description
	`->add fc-connection MyNewProfile` Adds a new FC SAN connection and uses the next available fabric
	`->add fc-connection MyNewProfile AddressType=Factory-Default` Adds a new FC SAN connection and uses factory-default addresses
	`->add fc-connection MyNewProfile AddressType=User-Defined PortWWN=50:06:0B:00:00:C2:62:00 NodeWWN=50:06:0B:00:00:c2:62:01` Adds a new FC SAN connection and provides user-defined WWN addresses

Item	Description
`remove fc-connection`	Remove the last FC connection from an existing server profile.
Syntax	`remove fc-connection <ProfileName>`
Parameter	
`ProfileName (required)`	The name of an existing profile from which the last FC connection is to be removed
Example	
	`->remove fc-connection MyProfile` Removes an FC connection from a profile

Item	Description
`set fc-connection`	Modify an existing FC SAN connection.
Syntax	`set fc-connection <ProfileName> <Port> [Fabric=<FabricName>] [Speed=<Auto|1Gb|2Gb|4Gb|8Gb|Disabled>] [BootPriority=<priority>] [BootPort=<portName>] [BootLun=<LUN>]`
Parameters	
`ProfileName (required)`	The name of the server profile that contains the connection to modify
`Port (required)`	The port number of the connection being modified
Properties	
`Fabric (optional)`	The name of the FC SAN fabric to associate with the connection. The fabric being specified should be associated with the same bay as the FC connection. A blank string makes the FC connection unassigned.
`Speed (optional)`	The port speed of the FC SAN connection. Valid values include "Auto", "8Gb", "4Gb", "2Gb", "1Gb", and "Disabled". Speed restrictions: For the HP 4Gb VC-FC Module and HP Virtual Connect 4Gb FC Module, supported speed values include "Auto","1Gb","2Gb", and "4Gb", and "Disabled". If the value is set to 8Gb, the speed is auto-negotiated by Virtual Connect.
`BootPriority (optional)`	Controls whether the FC HBA port is enabled for SAN boot and affects the BIOS boot order. Valid values include "BIOS", "Primary", "Secondary", and "Disabled".

Item	Description
`BootPort (optional)`	The target WWPN of the controller interface on the Fibre Channel storage target. The port name is a 64-bit identifier in the format NN:NN:NN:NN:NN:NN:NN:NN, where N is a hexadecimal number.
`BootLun (optional)`	The LUN of the volume used for SAN boot. Valid values include an integer from 0 to 255 or 16 hex digits (HP-UX only).
Examples	
	`->set fc-connection MyProfile 1 Fabric=SAN_5` Changes the fabric of an FC SAN fabric connection
	`->set fc-connection RedProfile 2 Fabric=""` Sets a FC SAN fabric connection to "Unassigned"
	`->set fc-connection BlueProfile 1 Fabric=SAN_7` Changes the FC SAN fabric of an FC SAN connection
	`->set fc-connection BlueProfile 1 Speed=4Gb` Changes the port speed of an FC SAN connection
	`->set fc-connection BlueProfile 1 BootPriority=Primary BootPort=50:06:0B:00:00:C2:62:00 BootLun=5` Changes the SAN boot priority and sets additional boot parameters

Item	Description
`show fc-connection`	Display the FC SAN connections associated with the server profiles.
Syntax	`show fc-connection [<ConnectionID>]`
Parameter	
`ConnectionID (optional)`	The ID of an existing FC SAN connection. The ID format is <ProfileName:Port>. <ProfileName:*> can be used to display all the FC SAN connections of a profile. '*' displays all the FC SAN connections existing in the domain.
Examples	
	`->show fc-connection` Displays all FC SAN connections existing in the domain
	`->show fc-connection Profile1:*` Displays FC SAN connections of profile Profile1
	`->show fc-connection Profile1:1` Displays a specific FC SAN connection of profile Profile1

firmware

Display the Virtual Connection firmware version.

Support actions: `help, show`

`show firmware`	Display the firmware information for all interconnect modules in the domain.
Syntax	`show firmware`

Examples	
	`->show firmware` Displays a summary listing of all firmware
	`->show firmware *` Displays a detailed listing of all firmware

To update firmware, use the HP BladeSystem c-Class Virtual Connect Support Utility. For more information on installing the firmware, see the HP BladeSystem c-Class Virtual Connect Support Utility documentation on the HP website (http://www.hp.com/go/bladesystem/documentation).

igmp

Manage Ethernet IGMP Snooping settings.

Supported actions: `help, set, show`

Item	Description
`set igmp`	Modify Ethernet IGMP Snooping settings.
Syntax	`set igmp [Enabled=<true|false>] [Timeout=<interval>]`
Properties	
`Enabled (optional)`	Enables or disables IGMP Snooping. Valid values include "true" and "false".
`Timeout (optional)`	The idle timeout interval (in seconds) for IGMP Snooping. Valid values include integers from 1-3600. The default IGMP idle timeout is 260 seconds.
Examples	
	`->set igmp Enabled=true` Enables IGMP Snooping
	`->set igmp Enabled=true Timeout=30` Enables IGMP Snooping and sets the idle timeout

Item	Description
`show igmp`	Display Ethernet IGMP Snooping settings.
Syntax	`show igmp`
Example	
	`->show igmp` Displays IGMP Snooping settings

interconnect

Manage I/O interconnect modules.

Supported actions: `help, remove, show`

Item	Description
`remove interconnect`	Remove an interconnect module from the domain. Normally this command is used if a module has been physically removed from the enclosure. To be removed, the module must not be currently in use by any element in the domain.

Item	Description
Syntax	`remove interconnect <ModuleID|*>`
Parameter	
`ModuleID(required)`	The ID of the module to remove. The ID format is `<EnclosureID>:<BayNumber>`. To display a list of the IDs corresponding to modules in the domain, use the `show interconnect` command.
Examples	
	`->remove interconnect enc0:2` Removes a specific interconnect module (bay 2) from the domain
	`->remove interconnect *` Removes all interconnect modules from the domain that are not present physically in any enclosure
	`->remove interconnect enc0:*` Removes all interconnect modules that are not present physically in a specific enclosure
	->remove interconnect *:2 **Removes interconnect modules (bay 2) from the domain that are not physically present in all enclosures**

Item	Description
`show interconnect`	Display all interconnect modules known to exist in the domain.
Syntax	`show interconnect [<ModuleID>|*]`
Property	
`ModuleID (optional)`	The ID of the interconnect module. "*" displays detailed view of all the modules in the VC domain. If not specified, a summary output of all the modules appears.
Examples	
	`->show interconnect` Displays a summary listing of all interconnect modules
	`->show interconnect *` Displays detailed information for all interconnect modules
	`->show interconnect *:5` Displays detailed information for all enclosures with interconnect modules in interconnect bay number 5
	`->show interconnect enc0:*` Displays interconnect modules in all bays of a specific enclosure
	`->show interconnect enc0:3` Displays detailed information on a specific interconnect module in interconnect bay 3 of the primary enclosure

ldap

Manage Virtual Connect directory server authentication settings.

Supported actions: `help, set, show`

Item	Description
`set ldap`	Modify and test the Virtual Connect LDAP directory server authentication settings.
Syntax	`set ldap [-test] [Enabled=<true|false>] [LocalUsers=<enabled|disabled>] [NtAccountMapping=<enabled|disabled>] [ServerAddress=<IP Address/DNS name>] [SslPort=<portNum>] [SearchContext1=<string>] [SearchContext2=<string>] [SearchContext2=<string>]`
Option	
`Test (optional)`	Tests the LDAP configuration without applying changes
Properties	
`Enabled (optional)`	Enables or disables LDAP authentication. Valid values include "true" and "false".
`LocalUsers (optional)`	Enables or disables local user authentication. Valid values include "Enabled" and "Disabled". WARNING: Disabling local users without correctly configuring LDAP authentication first may result in not being able to log on. Enabling and disabling local user authentication requires you to be logged in as an LDAP user. This property cannot be modified if logged in as a local user.
`NtAccountMapping (optional)`	Enables or disables Microsoft® Windows NT® account mapping. This capability enables you to enter "domain\username". Valid values include "Enabled" and "Disabled".
`SearchContext1 (optional)`	First searchable path used to locate the user when the user is trying to authenticate using directory services.
`SearchContext2 (optional)`	Second searchable path used to locate the user when the user is trying to authenticate using directory services.
`SearchContext3 (optional)`	Third searchable path used to locate the user when the user is trying to authenticate using directory services.
`ServerAddress (optional)`	The IP address or host name of the LDAP server used for authentication
`SslPort (optional)`	The port to use for LDAP communication. Valid values include a valid port number between 1 and 65535. The default port number is 636.
Examples	
	`->set ldap -test Enabled=true ServerAddress=192.168.0.27` Tests the directory service changes without applying
	`->set ldap Enabled=true ServerAddress=192.168.0.124 SslPort=636 SearchContext1="ou=users,dc=company,dc=com"` Enables directory services authentication for users

Item	Description
`show ldap`	Display the Virtual Connect LDAP authentication settings.
Syntax	`show ldap`
Example	

Item	Description
	->show ldap Displays LDAP information

ldap-certificate

View and upload LDAP certificates from a remote FTP server.

Supported actions: help, load, remove, show

Item	Description
load ldap-certificate	Download an LDAP Certificate from a remote FTP server and apply it to the VC domain.
Syntax	load ldap-certificate Address=<ftp://user:password@ipaddress> Filename=<name>
Properties	
Address (required)	A valid IP address or host name of the FTP server, including user name and password
Filename (required)	The name of the certificate file on the server.
Example	
	->load ldap-certificate Address=ftp://user:password@192.168.10.12 filename=/new-ldap.crt Downloads LDAP certification from the remote FTP server

Item	Description
remove ldap-certificate	Remove an existing LDAP certificate.
Syntax	remove ldap-certificate <SerialNumber | *>
Parameter	
SerialNumber (required)	The serial number of an existing LDAP certificate, or "*" to remove all the configured LDAP certificates.
Examples	
	->remove ldap-certificate B4:02:C0:29:B5:E5:B4:81 Removes an existing LDAP certificate by serial number
	->remove ldap-certificate * Removes all LDAP certificates

Item	Description
show ldap-certificate	Display LDAP certificate information.
Syntax	show ldap-certificate [<SerialNumber> | *]
Parameter	
SerialNumber (optional)	The serial number of an existing LDAP certificate in a colon format. "*"displays detailed output of all the LDAP certificates in the VC domain. If

Item	Description
	not specified, then displays summary output of all the LDAP certificates.
Examples	
	`->show ldap-certificate` Displays LDAP certificate details
	`->show ldap-cerificate *` Displays detailed information for all LDAP certificates
	`->show ldap-certificate B4:02:C0:29:B5:E5:B4:81` Displays detailed information for a specific LDAP certificate

ldap-group

Manage Virtual Connect directory groups.

Supported actions: `add, help, remove, set, show`

Item	Description
`add ldap-group`	Add a new directory group to the directory services configuration.
Syntax	`add ldap-group <GroupName> [Description=<string>] [Privileges=domain,server,network,storage]`
Parameters	
`GroupName (required)`	The name of the LDAP directory group to add
`Description (optional)`	An informational description for the new group to be added
`Privileges (optional)`	A set of one or more privileges for the group. Valid values include any combination of "domain", "server", "network" , and "storage".
Example	
	`->add ldap-group MyNewGroup Description="Test Group" Privileges=domain,server` Adds a new directory group

Item	Description
`remove ldap-group`	Remove an existing directory group.
Syntax	`remove ldap-group <GroupName|*>`
Parameter	
`GroupName (required)`	The name of an existing directory group to be removed, or "*" to remove all LDAP groups
Examples	
	`->remove ldap-group MyGroup` Removes a directory group
	`->remove ldap-group *` Removes all directory groups

Item	Description
`set ldap-group`	Modify the properties of an existing directory group.
Syntax	`set ldap-group <GroupName> [Description=<description>] [Privileges=<privileges>]`
Parameter	
`GroupName (required)`	The name of an existing group to modify
Properties	
`Description (optional)`	A user-friendly description for the group
`Privileges (optional)`	A set of one or more privileges for the group. Valid values include any combination of "domain", "server", "network", and "storage".
Example	
	`->set ldap-group MyGroup Description="Test Group" Privileges=domain,server,network` Modifies a directory group description and privileges

Item	Description
`show ldap-group`	Display the existing directory groups.
Syntax	`show ldap-group [<GroupName>|*]`
Parameter	
`GroupName (optional)`	The name of an existing LDAP group in the domain. If "*" is specified, then all LDAP groups appear. The default behavior, if not specified, is to display a summary of all groups.
Examples	
	`->show ldap-group` Displays a summary listing of all LDAP groups
	`->show ldap-group MyGroup` Displays detailed information for a specific LDAP group
	`->show ldap-group *` Displays detailed information for all LDAP groups

log-target

Manage remote log destination settings.

Supported actions: `add, help, remove, set, show, test`

Item	Description
`add log-target`	Add a new remote log destination.
Syntax	`add log-target <Destination=IpAddress|DNS> [Severity=<Critical|Error|Warning|Info>] [Transport=<TCP|UDP>] [Port=<1-65535>] [Security=<None|STunnel>] [Format=<RFC3164|ISO8601>] [State=<Enabled|Disabled>]`

Item	Description
Properties	
`Destination (required)`	The IpAddress or the DNS of the remote log destination that has been configured.
`Severity (optional)`	Severity of the log messages that should be sent to the specified destination. Valid values include "Critical", "Error", "Warning", and "Info". The default value is "Info".
`Transport (optional)`	The transport protocol to be used for sending the log messages to the destination. Valid values include "TCP" and "UDP". The default value is "UDP".
`Port (optional)`	The port to be used on the destination to send the log messages. Valid values include 1 to 65536. The default value is 514.
`Security (optional)`	Secure transmission of the log messages. Valid values include "None" and "STunnel". The default value is "None", and no encryption is used during transmission. The "STunnel" option can be used only if the transport protocol used is TCP.
`Format (optional)`	The timestamp format for the log messages. Valid values include "RFC3164" (Nov 26 13:15:55) and "ISO8601" (1997-07-16T19:20:30+01:00). The default value is "RFC3164".
`State (optional)`	Enables or disables the remote log destination. Valid values include "Enabled" and "Disabled". The default value is "Disabled".
Example	
	`->add log-target Destination=192.168.2.1 Port=600 Format=ISO8601 State=Enabled` Adds log-target 192.168.2.1

Item	Description
`remove log-target`	Remove an existing remote logging destination.
Syntax	`remove log-target <ID>`
Property	
`ID (required)`	The index of the remote log destination to be deleted
Example	
	`->remove log-target 3` Removes log-target index number 3

Item	Description
`set log-target`	Modify the properties of an existing remote log destination.
Syntax	`set log-target <ID> [Destination=<IpAddress|DNS>] [Severity=<Critical|Error|Warning|Info>] [Transport=<TCP|UDP>] [Port=<1-65535>] [Security=<None|STunnel>] [Format=<RFC3164|ISO8601>] [State=<Enabled|Disabled>]`
Parameter	
`ID (required)`	The index of the remote log destination whose configuration needs to be

Item	Description
	modified
Properties	
`Destination (optional)`	The IpAddress or the DNS of the remote log destination that has been configured
`Severity (optional)`	Severity of the log messages that should be sent to the specified destination. Valid values include "Critical", "Error", "Warning", and "Info". The default value is "Info".
`Transport (optional)`	The transport protocol to be used for sending the log messages to the destination. Valid values include "TCP" and "UDP". The default value is "UDP".
`Port (optional)`	The port to be used on the destination to send the log messages. Valid values include: 1 to 65536. The default value is 514.
`Security (optional)`	Secure transmission of the log messages. Valid values include "None" and "STunnel". The Default value is "None", and no encryption is used during transmission. The "STunnel" option can be used only if the transport protocol used is TCP.
`Format (optional)`	The timestamp format for the log messages. Valid values include "RFC3164" (Nov 26 13:15:55) and "ISO8601" (1997-07-16T19:20:30+01:00). The default value is "RFC3164".
`State (optional)`	Enables or disables the remote log destination. Valid values include "Enabled" and "Disabled". The default value is "Disabled".
Examples	
	`->set log-target 1 Severity=Error Transport=TCP Security=STunnel` Modifies log-target index number 1
	`->set log-target 1 Destination=192.168.3.1` Modifies log-target at index 3 and modifies the IP address to a new one

Item	Description
`show lot-target`	Display the remote log destination settings.
Syntax	`show log-target [<ID|*>]`
Property	
`ID (optional)`	The index of the remote log destination whose detailed configuration needs to be viewed. '*' displays detailed information of all the remote log destinations.
Example	
	`->show log-target` Displays all log destination settings

Item	Description
`test log-target`	Send a test message to all enabled remote log destinations.
Syntax	`test log-target`

Item	Description
Example	
	`->test log-target` Sends a test message all log-targets

mac-cache

Manage Ethernet MAC Cache failover settings.

Supported actions: `help, set, show`

Item	Description
`set mac-cache`	Modify Ethernet MAC Cache failover settings.
Syntax	`set mac-cache [Enabled=<true|false>] [Refresh=<interval>]`
Properties	
`Enabled (optional)`	Enables or disables MAC cache failover. Valid values include "true" and "false".
`Refresh (optional)`	The refresh interval for the MAC Cache (in seconds). Valid values include integers from 1-30. The default refresh interval is 5 seconds.
Examples	
	`->set mac-cache Enabled=true` Enables MAC Cache Failover
	`->set mac-cache Enabled=true Refresh=10` Enables MAC Cache Failover and sets the refresh interval

Item	Description
`show mac-cache`	Display Ethernet MAC Cache failover settings.
Syntax	`show mac-cache`
Example	
	`->show mac-cache` Displays Ethernet MAC Cache failover settings

network

Manage Virtual Connect Ethernet networks.

Supported actions: `add, help, remove, set, show`

Item	Description
`add network`	Create a new Ethernet Network. After the network has been created, uplink ports can be added if the network is not using a shared uplink port set. The SmartLink property is no longer supported during the creation of the network. If specified, it will be ignored. To configure the SmartLink attribute, use the `set network` command.
Syntax	`add network <NetworkName> [-quiet] [UplinkSet=<UplinkSetName> VLanID=<VLanID>] [State=<Enabled|Disabled>] [NativeVLAN=<Enabled|Disabled>] [Private=<Enabled|Disabled>]`

Item	Description
	[ConnectionMode=<Auto|Failover>] [VLanTunnel=<Enabled|Disabled>] [PrefSpeedType=<Auto|Custom>] [PrefSpeed=<100Mb-10Gb in 100Mb increments] [MaxSpeedType=<UnRestricted|Custom>] [MaxSpeed=<100Mb-10Gb in 100Mb increments>]
Parameter	
NetworkName (required)	The unique name of the new network to create
Option	
Quiet	Suppresses user confirmation prompts during network creation and modification. This option is used mainly in automated scripting scenarios.
Properties	
UplinkSet (optional)	The name of an existing shared uplink port set to use with this new network. If this property is specified, then a valid VLAN ID must also be provided. The limit is 32 networks per shared uplink set.
VLanID (optional)	The VLAN ID associated with the network (used with shared uplink port set only). The VLAN ID is a valid number between 1 and 4094.
State (optional)	Enables or disables the network. Valid values are "Enabled" and "Disabled". The default value is "Enabled".
NativeVLAN (optional)	Enables or disables the network to act as a native VLAN. Valid values are "Enabled" and "Disabled". The default value is "Disabled". This property can be specified only if the network is a shared network.
Private (optional)	Enables or disables the network to act as a private network. Valid values are "Enabled" and "Disabled". The default value is "Disabled".
ConnectionMode (optional)	Specifies the connection type that is formed when multiple ports are added to the network. Valid values include "Auto" and "Failover". The default value is "Auto".
VLanTunnel (optional)	Enables or disables VLAN tag tunneling. If enabled, VLAN tags are passed through the domain without any modification. If disabled, all tagged frames are discarded. If multiple networks are configured on any server port, this option cannot be modified.
PrefSpeedType (optional)	Default connection speed for any Ethernet connection attached to this network. Valid values include "Auto" and "Custom". "Custom" enables the user to configure the preferred speed. The default value is "Auto".
PrefSpeed (required if PrefSpeedType is "Custom")	The connection speed for any Ethernet connection attached to this network. Valid values range from 100Mb to 10Gb in 100Mb increments.
MaxSpeedType (Optional)	The maximum connection speed for any Ethernet connection attached to this network. Valid values include "Unrestricted" and "Custom". "Custom" enables the user to configure the preferred speed. The default value is "Unrestricted".
MaxSpeed (required if MaxpeedType is "Custom")	The maximum connection speed for any Ethernet connection attached to this network. Valid values range from 100Mb to 10Gb in 100Mb increments.
Examples	
	->add network MyNewNetwork Creates a new network, and then adds it to the domain
	->add network MyNewNetwork2 UplinkSet=MyUplinkSet VLanID=145 Creates a new network and uses a shared uplink port set

Item	Description
	`->add network Network1 Private=Enabled` Configures a private network when adding a new network
	`->add network Network1 UplinkSet=Uplinkset1 VLANID=100 NativeVLAN=Enabled` Creates a new network with a shared uplinkset and tags it as Native VLAN
	`->add network Network1 ConnectionMode=Failover` Creates a new network and sets the connection mode as failover
	`->add network Network1 VLanTunnel=Enabled` Creates a new network and enables VLAN tunneling
	`->add network Network1 PrefSpeedType=Custom PrefSpeed=4000 MaxSpeedType=Custom MaxSpeed=6000` Creates a new network with a preferred connection speed of 4Gb and maximum connection speed of 6Gb

Item	Description
`remove network`	Remove a network from the domain. To remove a network, it must not be in use by any server profiles.
Syntax	`remove network <NetworkName | *>`
Parameter	
`NetworkName (required)`	The name of an existing network in the domain. A network name of "*" removes all networks.
Examples	
	`->remove network MyNetwork` Removes a network
	`->remove network *` Removes all networks

Item	Description
`set network`	Modify an existing Ethernet network.
Syntax	`set network <NetworkName> [-quiet] [Name=<NewName>] [State=<Enabled|Disabled>] [SmartLink=<Enabled|Disabled>][NativeVLAN=<Enabled|Disabled>] [Private=<Enabled|Disabled>] [VlanId=<New VLanId>] [ConnectionMode=<Auto|Failover>] [VLanTunnel=<Enabled|Disabled>] [PrefSpeedType=<Auto|Custom>] [PrefSpeed=<100Mb-10Gb in 100Mb increments>] [MaxSpeedType=<UnRestricted|Custom>] [MaxSpeed=<100Mb-10Gb in 100Mb increments>]`
Parameter	
`NetworkName (required)`	The name of an existing network to modify
Option	
`Quiet (optional)`	Suppresses user confirmation prompts during network creation and modification. This option is used mainly in automated scripting scenarios.
Properties	
`Name (optional)`	The new name of the network
`State (optional)`	Enables or disables the network. Valid values are "Enabled" and "Disabled".

Item	Description
SmartLink (optional)	Enables or disables the SmartLink capability for a port. Valid values include "Enabled" and "Disabled". SmartLink cannot be modified unless one or more ports are added to the network.
NativeVLAN (optional)	Enables or disables the network to act as a native VLAN. Valid values are "Enabled" and "Disabled". The default value is "Disabled". This property can be configured only if it is applied to a shared network.
Private (optional)	Enables or disables the network to act as a private network. Valid values are "Enabled" and "Disabled". The default value is "Disabled".
VLanID (optional)	Modifies the VLAN ID of the network if it belongs to a shared uplink set that has not been configured.
ConnectionMode (optional)	Specifies the connection type that is formed when multiple ports are added to the network. Valid values include "Auto" and "Failover". The default value is "Auto".
VLanTunnel (optional)	Enables or disables VLAN tag tunneling. If enabled, VLAN tags are passed through the domain without any modification. If disabled, all tagged frames are discarded. If multiple networks are configured on any server port, this option cannot be modified.
PrefSpeedType (Optional)	Default connection speed for any Ethernet connection attached to this network. Valid values include "Auto" and "Custom". "Custom" enables the user to configure the preferred speed. The default value is "Auto".
PrefSpeed (Required if PrefSpeedType is 'Custom')	The connection speed for any Ethernet connection attached to this network. Valid values range from 100Mb to 10Gb in 100Mb increments.
MaxSpeedType (Optional)	Maximum connection speed for any Ethernet connection attached to this network. Valid values include "Unrestricted" and "Custom". "Custom" enables the user to configure the preferred speed. The default value is "Unrestricted".
MaxSpeed (required if MaxpeedType is "Custom)	The maximum connection speed for any Ethernet connection attached to this network. Valid values range from 100Mb to 10Gb in 100Mb increments.
Examples	
	`->set network MyNetwork State=Disabled` Disables an existing network named "MyNetwork"
	`->set network Blue Name=Red` Changes the name of an existing network from "Blue" to "Red"
	`->set network GreenNetwork SmartLink=Enabled` Enables the SmartLink feature on a specific network
	`->set network network1 NativeVLAN=Disabled` Disables the network native VLAN tagging
	`->set network network1 Private=Disabled` Disables the private network property
	`->set network Network1 Private=Enabled` Enables a private network
	`->set network Network1 VlanId=150` Changes the VLAN ID of a network associated with a shared uplink set
	`->set network Network1 VLanTunnel=Enabled` Enables VLAN tunneling on the network

Item	Description
	->set network Network1 PrefSpeedType=Custom PrefSpeed=4000 MaxSpeedType=Custom MaxSpeed=6000 Modifies network to preferred connection speed of 4Gb and maximum connection speed of 6Gb

Item	Description
show network	Display all Ethernet networks in the domain.
Syntax	show network [<NetworkName> | *]
Parameter	
NetworkName (optional)	Name of an existing network in the VC domain. "*" displays a detailed view of all the networks. If not specified, a summary view of the networks is displayed.
Examples	
	->show network Displays a summary listing of all networks
	->show network * Displays detailed information for all networks
	->show network MyNetwork Displays detailed information for a specific network

port-monitor

Manage port monitor configuration.

Supported actions: help, add, remove, set, show

Item	Description
add port monitor	Add a new network analyzer port and other ports to be monitored.
Syntax	add port-monitor [AnalyzerPort=<PortID>] [Speed=<Auto|10Mb|100Mb|1Gb|10Gb|Disabled>] [Duplex=<Auto|Half|Full>] [MonitorPort=<PortID>] [Direction=<ToServer|FromServer|Both>]
Properties	
AnalyzerPort (optional)	The uplink port that is used for monitoring network traffic. Only one port can be configured as the analyzer port. After a port has been allocated to port monitoring, it is not available for use in VC networks and shared uplink sets. The format of the network analyzer port is <EnclosureID>:<InterconnectBay>:<PortNumber>. If the enclosure ID is not specified, the default enclosure is the local enclosure where the domain resides.
Speed (optional)	The port speed for the network analyzer port. Valid values include "Auto", "10Mb", "100Mb", "1Gb", "10Gb", and "Disabled". The default value is "Auto". If there is no connector present on the analyzer port, only "Auto" and "Disabled" can be configured as a possible speed. Speed restrictions apply.

Item	Description
Duplex (optional)	The duplex mode of the network analyzer port. Valid values include "Auto", "Half", and "Full". The default value is "Auto".
MonitorPort (optional)	The server port to be monitored. The format of the monitored port is <EnclosureID>:<DeviceBay>:<PortNumber>. If the enclosure ID is not specified, the default enclosure is the local enclosure. The ID for the monitor port can be referenced from the ID column in the output of the show server-port command.
Direction (optional)	The direction of network traffic on the port being monitored. Valid values include "ToServer", "FromServer", and "Both".
Example	
	->add port-monitor AnalyzerPort=enc0:1:4 Speed=1Gb Duplex=full MonitorPort=enc0:5:4 Direction=FromServer Adds a new network analyzer port and a server port to be monitored

Item	Description
remove port-monitor	Remove ports from a port monitor configuration. Removing the network analyzer port causes port monitoring to be disabled automatically.
Syntax	remove port-monitor AnalyzerPort=<PortID|*> MonitorPort=<PortID|*>
Properties	
AnalyzerPort	The network analyzer port to be removed. "*" removes all the network analyzer ports from the configuration.
MonitorPort	The monitor port to be removed. "*" removes all the monitor ports from the port monitor configuration.
Examples	
	->remove port-monitor AnalyzerPort=enc0:3:1 Removes the network analyzer from the configuration
	->remove port-monitor AnalyzerPort=* Removes all network analyzer ports from the configuration
	->remove port-monitor monitorPort=enc0:1:1 Removes a specific server port from the monitored port list
	->remove port-monitor monitorPort=* Removes all monitored ports

Item	Description
set port-monitor	Modify an existing port monitor configuration.
Syntax	set port-monitor [Enabled=<true|false>] [AnalyzerPort=<PortID>] [Speed=<Auto|10Mb|100Mb|1Gb|10Gb|Disabled>] [Duplex=<Auto|Half|Full>] [MonitorPort=<PortID>] [Direction=<ToServer|FromServer|Both>]
Properties	
Enabled (optional)	Enables or disables port monitoring. The network analyzer port must be

Item	Description
	configured properly before port monitoring can be enabled.
AnalyzerPort (optional)	The uplink port used for monitoring network traffic. The format of the network analyzer port is <EnclosureID>:<InterconnectBay>:<PortNumber>. If the enclosure ID is not specified, the default enclosure is the local enclosure.
Speed (optional)	The port speed for the network analyzer port. Valid values include "Auto", "10Mb", "100Mb", "1Gb", "10Gb", and "Disabled". The default value is "Auto". If there is no connector present on the analyzer port, only "Auto" and "Disabled" can be configured as a possible speed. Speed restrictions apply.
Duplex (optional)	The port duplex mode of the network analyzer port. Valid values include "Auto", "Half", and "Full". The default value is "Auto".
MonitorPort (required if the Direction property is being modified)	The server port to be monitored. The format of the monitored port is <EnclosureID>:<DeviceBay>:<PortNumber>. If the enclosure ID is not specified, the default enclosure is the local enclosure where the domain resides.
Direction (optional)	The direction of network traffic on the port being monitored. Valid values include "ToServer", "FromServer", and "Both".
Examples	
	->set port-monitor AnalyzerPort=enc0:3:1 Speed=1Gb Duplex=half Modifies network analyzer uplink port properties
	->set port-monitor MonitorPort=enc0:1:6 Direction=ToServer Modifies a monitored server port
	->set port-monitor Enabled=true Enables port monitoring
	->set port-monitor Enabled=false Disables port monitoring

Item	Description
show port-monitor	Display the Virtual Connect port monitor configuration.
Syntax	show port-monitor
Example	
	->show port-monitor Displays the port monitor configuration

profile

Manage server profiles.

Supported actions: add, assign, help, remove, set, show, unassign

Item	Description
add profile	Create a new server profile. After the profile has been created, the profile can then be configured using the "set" subcommand, and the additional network, fabric, and FCoE connections can also be added. The server profile can also be

Item	Description
	assigned to a device bay using the "assign" subcommand.
Syntax	`add profile <ProfileName> [-NoDefaultEnetConn] [-NoDefaultFcConn] [-NoDefaultFcoeConn] [SNType=<Factory-Default|User-Defined>] [SerialNumber=<serialnumber>] [UUID=<uuid>]`
Parameter	
`ProfileName`	The unique name of the new server profile to create
Options	
`NoDefaultEnetConn`	Do not add default Ethernet Network connections when creating the server profile.
`NoDefaultFcConn`	Do not add default FC SAN connections when creating the server profile.
`NoDefaultFcoeConn`	Do not add default FCoE SAN connections when creating the server profile.
Properties	
`SNType (Optional)`	The source of the serial number assignment to be used during the profile creation. If not specified, the serial number is assigned according to the Virtual connect default domain settings. Valid values include "Factory-Default" and "User-Defined".
`SerialNumber (required if the SNType is User-Defined)`	A custom user-defined serial number associated with the server profile. When the profile is assigned to a device bay that contains a server, the server inherits the virtual serial number. The user-defined serial number must start with the pattern VCX01.
`UUID (Optional)`	A unique 128-bit identifier for the virtual server ID. The format is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, where x is any alpha-numeric character. If no UUID is specified, then one is auto-generated. The UUID can be specified only if the SNType is User-Defined.
Examples	
	`->add profile MyNewProfile` Creates a new profile and adds it to the domain, using default connections and Virtual Connect default serial numbers
	`->add profile MyNewProfile2 -NoDefaultEnetConn` Creates a new profile without adding default Ethernet connections
	`->add profile MyNewProfile2 -NoDefaultFcConn` Creates a new profile without adding default FC connections
	`->add profile MyNewProfile2 -NoDefaultFcoeConn` Creates a new profile without adding default FCoE connections
	`->add profile MyNewProfile2 -NoDefaultEnetConn -NoDefaultFcConn` Creates a new profile without adding default Ethernet and FC connections
	`->add profile MyNewProfile2 -NoDefaultEnetConn -NoDefaultFcConn -NoDefaultFcoeConn` Creates a new profile without adding default Ethernet, FC, and FCoE connections
	`->add profile MyNewProfile SNType=User-Defined SerialNumber=VCX0113121` Creates a new profile and specifies a custom virtual serial number
	`->add profile MyNewProfile SNType=Factory-Default` Creates a new profile and uses the factory assigned serial number

Item	Description
	`->add profile MyNewProfile SNType=User-Defined SerialNumber=VCX0113121 UUID=15713c60-fcf2-11dc-a656-0002a5d5c51b` Creates a new profile and specifies a custom virtual serial number and UUID

Item	Description
`assign profile`	Assign a server profile to a device bay.
Syntax	`assign profile <ProfileName> <DeviceBay> [-PowerOn]`
Parameters	
`ProfileName (required)`	The unique name of the server profile to assign
`DeviceBay (required)`	The device bay to assign the profile to, in the format `<EnclosureID>:<DeviceBayNumber>` If EnclosureID is not specified, it defaults to the local enclosure. To assign a profile to a multi-blade server, <DeviceBay> must be a monarch bay.
Option	
`PowerOn`	Powers on the server after the profile has been assigned.
Example	
	`->assign profile MyProfile1 enc0:1` Assigns a profile to device bay 1 of the primary enclosure
	`->assign profile MyProfile1 enc0:5` Assigns a profile to a multi-blade server in bays 5-8 of the primary enclosure

Item	Description
`remove profile`	Remove one or more server profiles from the domain.
Syntax	`remove profile <ProfileName | *>`
Parameter	
`ProfileName (required)`	The name of an existing profile in the VC domain. "*" removes all the existing profiles.
Examples	
	`->remove profile MyProfile` Removes a server profile by name
	`->remove profile *` Removes all server profiles

Item	Description
`set profile`	Modify properties of an existing server profile.
Syntax	`set profile <ProfileName> [Name=<NewName>] [EFIState=absent]`
Parameter	
`ProfileName (required)`	The current name of the profile to modify
Properties	

Item	Description
`Name (required)`	The new name of the server profile
`EFIState (required)`	Specifies the presence or absence of EFI state information
Examples	
	`->set profile MyProfile Name=MyNewProfileName` Changes the name of a server profile
	`->set profile Profile1 EFIState=absent` Removes EFI partition block information from a profile

Item	Description
`show profile`	Display all server profiles that exist in the domain and a summary of the associated Ethernet, iSCSI, FC, and FCoE connections. To view detailed information for the connections, use the `show enet-connection`, `show iscsi-connection`, `show fc-connection`, and `show fcoe-connection` commands, respectively.
Syntax	`show profile [<ProfileName> | *]`
Parameter	
`ProfileName (optional)`	The name of an existing profile in the VC domain. "*" displays all the existing profiles. If not specified, a summary of all the profiles appears.
Examples	
	`->show profile` Displays a summary listing of all server profiles
	`->show profile *` Displays detailed information for all profiles
	`->show profile MyProfile` Displays detailed information for a specific profile

Item	Description
`unassign profile`	Unassign a server profile from a device bay.
Syntax	`unassign profile <ProfileName>`
Parameter	
`ProfileName (required)`	The name of a server profile that is currently assigned to a device bay
Example	`->unassign profile MyProfile1` Unassigns a server profile from a device bay

server

Manage server blades.

Supported actions: `help, poweroff, poweron, reboot, show`

Item	Description
`poweroff server`	Power off one or more physical servers.

Item	Description
Syntax	`poweroff server <ServerID|*> [-Force | -ForceOnTimeout] [-timeout=<timeout>]`
Parameter	
`ServerID (required)`	The reference ID of a physical server in the domain. The format of the server ID is `<EnclosureID:DeviceBay>`. If the Enclosure ID is not provided, then the primary or local enclosure is used by default. "*" powers off all servers in the domain. For a multi-blade server, the ServerID must be that of the monarch bay. This is the ID displayed by the `show server` command.
Options	
`Force`	Forces a power off operation without waiting for the OS to shutdown gracefully. This option should only be used as a last resort because it can cause potential data loss on the server.
`ForceOnTimeout`	Attempts a graceful shutdown, but if the server does not shut down within the timeout period (default is 60 seconds), then the server is forced to power off.
`Timeout`	Specifies the timeout period (in seconds) to wait for the operation to complete (per server). The default timeout is 60 seconds.
Examples	
	`->poweroff server enc0:2` Shuts down a specific server in device bay 2 of an enclosure with ID enc0
	`->poweroff server enc0:2 -Force` Forces a power off operation on a specific server (primary/local enclosure)
	`->poweroff server *` Powers off all servers in the domain
	`->poweroff server enc0:*` Powers off all servers in a specific enclosure
	`->poweroff server enc0:2 -ForceOnTimeout` Attempts a graceful shutdown, but forces a shutdown at the end of the timeout period
	`->poweroff server * -timeout=180` Shuts down all servers and specifies a custom timeout of 3 minutes
	`->poweroff server enc0:1` Powers off a specific multi-blade server that occupies bays 1-4 of the primary enclosure

Item	Description
`poweron server`	Power on one or more physical servers.
Syntax	`poweron server <ServerID|*> [-Timeout=<timeout>]`
Parameter	
`ServerID (required)`	The reference ID of a server in the domain. The format of the server ID is `<EnclosureID:DeviceBay>`. If the EnclosureID is not provided, then the primary or local enclosure is used by default. "*" powers on all servers in the domain. For a multi-blade server, the ServerID must be that of the monarch bay. This is the ID displayed by the `show server` command.
Option	

Item	Description
Timeout	The timeout period (in seconds) to wait for the operation to complete. The default timeout is 60 seconds.
Examples	
	`->poweron server 2` Powers on the specific server in bay 2 of the primary enclosure
	`->poweron server *` Powers on all servers in the domain
	`->poweron server enc0:*` Powers on all servers in a specific enclosure
	`->poweron server * -Timeout=120` Powers on all servers and specifies a custom timeout of 2 minutes
	`->poweron server enc0:1` Powers on a specific multi-blade server that occupies bays 1-4 of the primary enclosure

Item	Description
reboot server	Reboot one or more physical servers.
Syntax	`reboot server <ServerID|*> [-Force] [-ForceOnTimeout] [-timeout=<timeout>`
Parameter	
ServerID (required)	The reference ID of a server in the domain. The format of the server ID is `<EnclosureID:DeviceBay>`. If the Enclosure ID is not provided, then the primary or local enclosure (enc0) is used by default. "*" reboots all servers in the domain. For a multi-blade server, the ServerID must be that of the monarch bay. This is the ID displayed by the `show server` command.
Options	
Force	Forces a reboot operation without waiting for the OS to shut down gracefully. This option should be used only as a last resort because it can cause potential data loss on the server.
ForceOnTimeout	Attempts a graceful shutdown, but if the server does not shut down within the timeout period (default is 60 seconds), then the server is forced to reboot.
Timeout	Specifies the timeout period (in seconds) to wait for the operation to complete (per server). The default timeout is 120 seconds.
Examples	
	`->reboot server 2` Reboots the specific server in device bay 2 of the primary enclosure
	`->reboot server enc0:2 -force` Reboots a server using the force option
	`->reboot server * -ForceOnTimeout -timeout=180` Reboots all servers using the ForceOnTimeout option and a custom timeout
	`->reboot server *` Reboots all servers in the domain
	`->reboot server enc0:*` Reboots all servers in a specific enclosure

Item	Description
	`->reboot server enc0:1` Reboots a specific multi-blade server that occupies bayes 1-4 of the primary enclosure

Item	Description
`show server`	Display all servers in the domain.
Syntax	`show server <ServerID|*>`
Parameter	
`ServerID (optional)`	The reference ID of a server in the domain. The format of the server ID is `<EnclosureID:Bay>`. If the EnclosureID is not provided, then the primary or local enclosure is used by default. For a multi-blade server, the ServerID must be that of the monarch bay. This is the ID shown in the summary listing.
Examples	
	`->show server` Displays a summary listing of all servers
	`->show server *` Displays detailed information for all servers
	`->show server enc2:*` Displays detailed information for all servers in a specific enclosure
	`->show server enc0:4` Displays detailed information for the specific server in device bay 4 of an enclosure named "MyEnclosure"
	`->show server enc0:5` Displays detailed information for a specific multi-blade server that occupies bays 5-8 of the primary enclosure

serverid

Manage virtual Server ID configuration settings.

Supported actions: `help, set, show`

Item	Description
`set serverid`	Modifiy Virtual Server ID domain settings. The serial number attributes can be changed only in one of the following scenarios: • Virtual Server ID source is Factory-Default. • Virtual Server ID source is VC-Defined or User-Defined, but no profiles are using server IDs from this source. • Virtual Server ID source is User-Defined, and this range is being extended by lowering the start or increasing the end values.
Syntax	`set serverid Type=Factory-Default`
	`set serverid Type=VC-Defined [PoolID=<1-64>]`
	`set serverid Type=User-Defined Start=VCX01nnnnn End=VCX01nnnnn`
Properties	

Item	Description
`Type (required)`	The type of the virtual serial number source. When server profiles are created, the virtual serial numbers and UUID values are allocated from the specified pool source. Valid values include "Factory-Defined" (default), "VC-Defined", and "User-Defined".
`PoolID (optional)`	The VC-Defined Pool ID to be used. If not specified, the default Pool ID is 1. This property is only valid for VC-Defined-serial number types.
`Start (required if Type is User-Defined)`	The starting serial number in a user-defined range. This property is only valid for User-Defined serial number types. User-Defined serial number ranges should start with the pattern VCX01.
`End (required if Type is User-Defined)`	The ending serial number in a user-defined range. This property is only valid for User-Defined serial number types. User-Defined serial number ranges should start with the pattern VCX01.
Examples	
	`->set serverid Type=Factory-Default` Modifies virtual server ID settings to use factory default serial numbers
	`->set serverid Type=VC-Defined PoolId=5` Modifies virtual server ID settings to use VC-Defined serial numbers
	`->set serverid Type=User-Defined Start=VCX0000001 End=VCX0100010` Modifies virtual server ID settings to use a custom, User-Defined serial number range

Item	Description
`show serverid`	Display virtual server ID configuration properties.
Syntax	`show serverid`
Example	
	`->show serverid` Displays virtual server ID configuration properties

server-port

Display the physical server ports.

Supported actions: `help`, `show`

Item	Description
`show server-port`	Display physical server port information.
Syntax	`show server-port <PortID>`
Parameter	
`PortID (Optional)`	The reference of a port mapping ID. The PortID format is `EnclosureID:IOBay:Port`. The Port ID can be referenced from the ID column in the summary display. The detailed display shows any Flex NICs that might be associated with a server port.
Examples	

Item	Description
	->show server-port Displays a summary listing of all physical server ports
	->show server-port * Displays detailed information for all physical server ports
	->show server-port enc0:3:d2 Displays detailed information for a specific server port

server-port-map

Manage shared server downlink port mapping configuration

Supported actions: add, help, remove, set, show

Item	Description
add server-port-map	Add a new server port network mapping, and allow server ports to be shared among multiple VC Ethernet networks. This command cannot be used if the domain setting VLanTagControl is currently set to "Tunnel".
Syntax	add server-port-map <ConnectionId> <Network Name> [Uplinkset=<Uplink Set Name>] [VLanID=<VLan ID>] [Untagged=<true|false>]
Parameters	
ConnectionID (required)	The reference ID of an existing enet-connection associated with a profile and a server port. The format of the ConnectionId is <ProfileName:PortNumber>.
Network (required)	The name of a valid network to which the mapping will be added. A network can be configured once for every profile connection, and every profile connection can be configured for a maximum of 28 networks.
Properties	
Uplinkset (optional)	The name of the shared uplinkset to use with the server port mapping. If the domain setting SharedServerVLanId is set to "true", then the Uplinkset is a required value.
VLanID (optional)	The VLAN ID to be used for the mapping. Valid values include 1 to 4094. If the uplinkset name is specified, then the VLanID property should not be specified, because the server VLAN ID is forced to be same as the VLAN ID used when adding the network to the shared uplinkset.
Untagged (optional)	Enables or disables the network to handle untagged packets. Only one network in an Ethernet network connection can be made to handle untagged packets. The default value is "false". If a shared uplink set is being used, then the untagged network is the same as the native network, if present, but any other network can be configured to handle untagged packets.
Examples	
	->add server-port-map MyProfile:1 Network1 VLanID=100 Adds a new server port to dedicated network mapping
	->add server-port-map MyProfile:2 RedNetwork Uplinkset=MyUplinkSet1 Adds a new server port to shared network mapping
	->add server-port-map MyProfile:3 GreenNetwork

Item	Description
	`Uplinkset=MyUplinkset1 UnTagged=true` Adds a new server port to shared network and label it as untagged

Item	Description
`remove server-port-map`	Remove a server port network mapping. This command cannot be used if the domain setting VLanTagControl is set to "Tunnel".
Syntax	`remove server-port-map <ConnectionID | *> [<Network Name>]`
Parameters	
`ConnectionID (required)`	The reference ID of an existing enet-connection associated with a profile and a server port. The format of the ConnectionId is <ProfileName:PortNumber>. "*" removes all server-port-map configurations from the domain.
`Network (optional)`	The name of an Ethernet network on which the mapping exists
Examples	
	`->remove server-port-map MyProfile:1 RedNetwork` Removes a server port network mapping
	`->remove server-port-map MyProfile:1 *` Removes all server port network mappings from a profile
	`->remove server-port-map *` Removes all the server port mappings in the domain

Item	Description
`set server-port-map`	Modify an existing server port network mapping. This command cannot be used if the domain setting VLanTagControl is set to "Tunnel" or if the network is associated with a shared uplink port set.
Syntax	`set server-port-map <ConnectionID> <Network Name> [VLanID=<VLanID>] [UnTagged=<true|false>]`
Parameters	
`ConnectionID (required)`	The reference ID of an existing enet-connection associated with a profile and a server port. The format of the ConnectionId is <ProfileName:PortNumber>.
`Network (required)`	The name of a valid Ethernet network on which the mapping exists
Properties	
`VLanID (optional)`	The new VLAN ID to be used for the mapping server port to network. Valid values include 1 to 4094.
`Untagged (optional)`	Enables or disables the network to handle untagged packets. Only one network in an Ethernet network connection is allowed to handle untagged packets. The default value is "false". If a shared uplink set is being used, the untagged network is the same as the native network if present, but any network can also be configured to handle untagged packets. When changing a network untagged option from true to false, the user is required to provide a VLanID if the global option SharedServerVLanId is set to "false".
Examples	
	`->set server-port-map MyProfile:1 Network1 VLanId=100`

Item	Description
	Modifies the VLAN ID of an existing server port network mapping
	`->set server-port-map MyProfile:1 Network1 Untagged=true` Modifies the existing server port network mapping to handle untagged packets

Item	Description
`show server-port-map`	Display a server port network mapping. This command cannot be used if the domain setting, VLanTagControl, is set to "Tunnel".
Syntax	`show server-port-map [<ConnectionID> | *]`
Parameter	
`ConnectionID (optional)`	The reference ID of an existing enet-connection associated with a profile and a server port. The format of the ConnectionId is <ProfileName:PortNumber>.
Examples	
	`->show server-port-map` Lists all the server port mappings
	`->show server-port-map MyProfile:1` Displays the server port mapping for a profile
	`->show server-port-map *` Displays detailed output of all the server port mappings

snmp

View and modify the SNMP configuration for VC-Enet and VC-FC modules, and add, modify, and remove SNMP trap configurations related to trap destinations.

Supported actions: `set, show, help`

Item	Description
`set snmp`	Modify the VC SNMP configuration.
Syntax	`set snmp <Type> [ReadCommunity=<ReadCommunityString>] [SystemContact=<SystemContact>] [Enabled=<true|false>] [SmisEnabled=<true|false>]`
Parameter	
`Type (required)`	Indicates which SNMP configuration to modify. Valid values include "Enet" and "FC".
Properties	
`ReadCommunity (optional)`	Read-Only Community String for the SNMP configuration. The default value is "public". If the type is "Enet", the maximum length of the read community string is 39 characters. If the type is FC, the maximum length is 12 characters.
`SystemContact (optional)`	SNMP system contact information.
`Enabled (optional)`	Enables or disables the SNMP agent. The default value is "true". Valid values include "true" or "false".
`SmisEnabled (optional)`	Enables or disables SMIS. This property is valid only for VC-FC modules. The default value is "false". Valid values include "true" or "false".

Item	Description
Examples	
	`->set snmp enet ReadCommunity=mydatacenter1 SystemContact=admin@datacenter1.com Enabled=true` Enables the SNMP agent for VC-Enet modules and supplies a community string
	`->set snmp fc ReadCommunity=mydatacenter SystemContact=FcAdmin Enabled=true` Enables the SNMP agent for VC-FC modules

Item	Description
`show snmp`	Display the SNMP configuration settings for the VC domain.
Syntax	`show snmp [Type]`
Parameter	
`Type (optional)`	Indicates the type of SNMP configuration to display. If the type is not specified, all VC SNMP configuration information appears. Valid values include "Enet" and "FC".
Examples	
	`->show snmp Enet` Displays SNMP configuration for VC-Enet modules only
	`->show snmp FC` Displays SNMP configuration for VC-FC modules only
	`->show snmp` Displays SNMP configuration for all modules

snmp-trap

Manage SNMP trap information

Supported actions: `add, help, remove, set, show, test`

Item	Description
`add snmp-trap`	Adds a new SNMP trap destination. Avoid using duplicate trap destinations. Setting duplicate trap destinations can result in duplicate traps being sent to the same destination, or only one of the trap destinations being configured.
Syntax	`add snmp-trap <Name> Address=<trap destination address> [Community=<community name string>][Format=<SNMPv1|SNMPv2>][Severity=<trap severity|All|None>][DomainCategories=<domain trap category|All|None>][EnetCategories=<enet trap category|All|None>][FcCategories=<fc trap category|All|None>]`
Parameter	
`Name (required)`	A unique name for the new trap being added
Properties	
`Address (required)`	IPv4 address or DNS name for the trap destination
`Community (optional)`	The SNMP community name string for the specified trap. The default value is "public" if not specified. For VC-Enet modules, the maximum string length is 39.

Item	Description
	For VC-FC modules, the maximum string length is 24.
`Format`	Format of the new trap. Valid values are "SNMPv1" and "SNMPv2". The default is "SNMPv1" if not specified.
`Severities`	Trap severities to send to the destination. Valid values are "Normal", "Unknown", "Info", "Warning", "Minor", "Major", "Critical", "All", and "None". Multiple severities can be provided, separated by commas. The default severity is "None".
`DomainCategories`	The Virtual Connect Domain trap categories to send to the destination. Valid values are "Legacy", "DomainStatus", "NetworkStatus", "FabricStatus", "ProfileStatus", "ServerStatus", "EnetStatus", FcStatus", "All", and "None". Multiple categories can be specified, separated by commas.
`EnetCategories`	The Virtual Connect Ethernet trap categories to send to the destination. Valid values are "PortStatus", "PortThreshold", "Other", "All", and "None". Multiple categories can be specified, separated by commas.
`FcCategories`	The Virtual Connect Fibre Channel trap categories to send to the destination. Valid values are "PortStatus", "Other", "All", and "None". Multiple categories can be specified, separated by commas.
Examples	
	`->add snmp-trap EnetManagementStation Address=192.112.34.10 Community=private Format=SNMPv1 Severity=Normal,Critical EnetCategories=Other` Adds a new trap destination for VC-Enet modules
	`->add snmp-trap FcManagementStation Address=192.112.72.3 Community=private Format=SNMPv1 FcCategories=Other` Adds a new trap destination for VC-FC modules
	`->add snmp-trap MyTrap Address=192.112.66.12` Adds a new trap using typical defaults
	`->add snmp-trap MyTrap Address=192.112.42.5 Severity=All FcCategories=All DomainCategories=All` Adds a trap with all severity and category properties set. Severities are allowed even though FC Categories are set; the severities will be applied to the Domain Categories.

Item	Description
`remove snmp-trap`	Removes a previously configured SNMP trap destination
Syntax	`remove snmp-trap <Name | *>`
Parameter	
`Name (required)`	The name of the trap destination to be removed. If "*" is specified, then all traps are removed.
Examples	
	`->remove snmp-trap MyTrap1` Removes an SNMP trap destination
	`->remove snmp-trap *` Removes all configured SNMP trap destinations

Item	Description
`set snmp-trap`	Modifies an existing SNMP trap destination
Syntax	`set snmp-trap <TrapName> [Name=<trap destination name>][Address=<trap destination address>][Community=<community name string>][Format=<SNMPv1 | SNMPv2>][Severity=<trap severity | All|None>][DomainCategory=<domain trap category | All|None>][EnetCategory=<enet trap category | All|None>][FcCategory=<fc trap category | All|None>]`
Parameter	
`TrapName (required)`	The name of the trap to be modified
Properties	
`Name`	New name of the trap
`Address (required)`	IPv4 address or DNS name for the trap destination
`Community (optional)`	The SNMP community name string for the specified trap. For VC-Enet modules, the maximum string length is 39. For VC-FC modules, the maximum string length is 24. If not specified, the default community name is "public".
`Format`	Format of the new trap. Valid values are "SNMP1v" and "SNMPv2". The default is "SNMPv1".
`Severity`	Trap severities to send to the destination. Valid values are "Normal", "Unknown", "Info", "Warning", "Minor", "Major", "Critical", "All", and "None". Multiple severities can be provided, separated by commas. The default severity is "None".
`DomainCategories`	The Virtual Connect Domain trap categories to send to the destination. Valid values are "Legacy", "DomainStatus", "NetworkStatus", "FabricStatus", "ProfileStatus", "ServerStatus", "EnetStatus", FcStatus", "All", and "None". Multiple categories can be specified, separated by commas.
`EnetCategories`	The Virtual Connect Ethernet trap categories to send to the destination. Valid values are "PortStatus", "PortThreshold", "Other", "All", and "None". Multiple categories can be specified, separated by commas.
`FcCategories`	The Virtual Connect Fibre Channel trap categories to send to the destination. Valid values are "PortStatus", "Other", "All", and "None". Multiple categories can be specified, separated by commas.
Examples	
	`->set snmp-trap MyTrap1 Community=public` Sets the trap community
	`->set snmp-trap MyTrap1 Severity=All FcCategories=None EnetCategories=None` Sets all trap severities, and also sets the Fibre Channel and Ethernet categories to none

Item	Description
`->show snmp-trap`	Displays the SNMP traps that have been configured
Syntax	`show snmp-trap [Name| *]`
Parameter	

Item	Description
`Name (optional)`	The name of the trap configuration to be displayed. If no trap name is specified, or "*" is entered, then all configured traps are displayed.
Examples	
	`->show snmp-trap MyTrap1` Displays the SNMP trap configuration for a single trap
	`->show snmp-trap *` Displays all configured SNMP traps

Item	Description
`->test snmp-trap`	Generates an SNMP test trap and sends it to all configured destinations. Traps participating in the test must be configured, at a minimum, with the following attributes: DomainCategories: DomainStatus Severity: Info
Syntax	`test snmp-trap`
Example	`->test snmp-trap` Generates an SNMP test trap and sends it to the configured destinations

ssh

Manage SSH configuration and information.

Supported actions: `help, load, remove, show`

Item	Description
`load ssh`	Transfer the SSH key from a remote FTP server and apply it to the Virtual Connect domain. A customized SSH key enables additional security for SSH clients that are allowed to access the domain configuration. If a new custom SSH key is applied, then the SSH clients must be configured correctly to have access.
Syntax	`load ssh Address=<ftp://user:password@ipaddress> FileName=<name>`
Properties	
`Address (required)`	The IP address or host name of an FTP server, with username and password
`FileName (optional)`	The name of the remote file containing the SSH key to transfer
Example	
	`->load ssh Address=ftp://user:password@192.168.10.12 FileName=/ssh_key.pub` Transfers the SSH key from the remote FTP server

Item	Description
`remove ssh`	Remove any custom SSH keys that have been applied.
Syntax	`remove ssh`

Item	Description
Example	
	`->remove ssh` Removes SSH keys

Item	Description
`show ssh`	Display the SSH key configuration.
Syntax	`show ssh`
Example	
	`->show ssh` Displays the SSH key configuration

ssl

Allow or disallow weak SSL encryption (browser/SOAP).

Supported actions: `set, show, help`

Item	Description
`set ssl`	Allow modifications to be made to the SSL configuration, and enable or disable string encryption for SSL communication with the web server.
Syntax	`set ssl Strength=[<All|Strong>]`
Property	
`Strength (required)`	The strength of the encryption cipher. Valid values include "All" and "Strong". The default value is "All".
Examples	
	`->set ssl strength=strong` Enables strong SSL encryption
	`->set ssl strength=all` Enables default SSL encryption settings (weak)

Item	Description
`show ssl`	Display SSL current configuration.
Syntax	`show ssl`
Example	
	`->show ssl` Displays SSL current configuration

ssl-certificate

View and upload the SSL certificate from a remote FTP server.

Supported actions: `help, load, show`

Item	Description
`load ssl-certificate`	Transfer an SSL Certificate from a remote FTP server and apply it to the Virtual Connect Manager web server. After a new SSL certificate is applied, the web server is reset.
Syntax	`load ssl-certificate Address=<ftp://user:password@ipaddress> Filename=<name>`
Properties	
`Address (required)`	A valid IP address or host name of the FTP server, with username and password
`Filename (required)`	The name of the certificate file on the remote FTP server
Example	
	`->load ssl-certificate Address=ftp://user:password@192.168.10.12 Filename=my-new-ssl.crt` Transfers a new custom SSL Certificate from the remote FTP server

Item	Description
`show ssl-certificate`	Display the Virtual Connect web server SSL certificate information.
Syntax	`show ssl-certificate [*]`
Examples	
	`->show ssl-certificate` Displays web server SSL Certificate details
	`->show ssl-certificate *` Displays detailed information of SSL certificate

ssl-csr

Transfer an SSL certificate signing request to a remote FTP server.

Supported actions: `help, save`

Item	Description
`save ssl-csr`	Generate and transfer an SSL certificate signing request (CSR) to a remote FTP server.
Syntax	`save ssl-csr address=<ftp://user:password@ipaddress> filename=<name>`
Properties	
`Address (required)`	A valid IP address or host name of the FTP server, with username and password
`Filename (required)`	The name of the file to which the generated SSL CSR will be stored on the FTP server. If not specified, the default file name will be "vc-ssl.csr".
Example	

Item	Description
	`->save ssl-csr address=ftp://user:password@192.168.10.12` Generates and transfers an SSL CSR to the remote FTP server
	`->save ssl-csr address=ftp://user:password@192.168.10.12 filename=new-ssl.csr` Generates and transfers an SSL CSR and save with a new filename

stackinglink

Display stacking link information and status.

Supported actions: `help, show`

Item	Description
`show stackinglink`	Display stacking links and their status.
Syntax	`show stackinglink`
Example	`->show stackinglink` Displays a summary listing of all stacking links and status

statistics

Manage statistics for interconnect module ports.

Supported actions: `help, reset, show`

Item	Description
`reset statistics`	Reset per-port statistics for the specified port ID.
Syntax	`reset statistics <PortID>`
Parameter	
`PortID (required)`	The port ID on which to reset statistics. The port ID must be in the format `<EnclosureID>:<BayNumber>:<PortLabel>` A listing of the possible uplink port IDs can be obtained by using the `show uplinkport` command.
Example	
	`->reset statistics enc0:3:1` Resets statistics for port 1 on interconnect module 3 of the primary enclosure.

Item	Description
`show statistics`	Display per-port statistics for the specified port ID.
Syntax	`show statistics <PortID>`
Parameter	
`PortID (required)`	The port ID on which to display statistics. The port ID must be in the format `<EnclosureID>:<BayNumber>:<PortLabel>`. FC downlink port statistics are not available. A listing of the possible uplink port IDs can be obtained by using the `show uplinkport` command.

Item	Description
Examples	
	`->show statistics enc0:5:X1` Displays statistics for uplink port X1 on interconnect module 3 of the primary enclosure.
	`->show statistics enc0:1:d3` Displays statistics for downlink port d3 on Ethernet interconnect module 1 of the primary enclosure.

status

View overall domain status information.

Supported actions: `help, show`

Item	Description
`show status`	Display the status of the domain and all components in the domain.
Syntax	`show status`
Example	`->show status` Displays domain status information

supportinfo

Generate and transfer a support information file to a remote FTP or TFTP server on the network.

Supported actions: `help, save`

Item	Description
`save supportinfo`	Generate and transfer a Virtual Connect Support Information file to a remote TFTP or FTP server.
Syntax	`save supportinfo address=<tftp://ipaddress | ftp://user:password@ipaddress>`
Parameter	
`Address (required)`	A valid IP address of a TFTP or FTP server, with user name and password (where required)
Examples	
	`->save supportinfo address=tftp://192.168.10.12` Saves a support information file to a remote TFTP server
	`->save supportinfo address=ftp://user:password@192.168.10.12` Saves a support information file to a remote FTP server

systemlog

View the Virtual Connect Manager system event log.

Supported actions: `help, show`

Item	Description
`show systemlog`	Display the Virtual Connect manager system log.
Syntax	`show systemlog [-Last=<n>] [-First=<n>] [-Pause=<n>]`
Options	
`Last`	Display the last `n` records. If this option is specified and no value is provided, the default is the last 10 records.
`First`	Display the first `n` records. If this option is specified and no value is provided, the default is the first 10 records.
`Pause`	Number of records to be viewed before prompting for key press. Valid values include numbers between 1 and 40.
Examples	
	`->show systemlog` Displays the entire system log
	`->show systemlog -pause=8` Displays the system log, eight records at a time
	`->show systemlog -first=12` Displays the first twelve records from the system log
	`->show systemlog -last=8` Displays the last eight records from the system log
	`->show systemlog -last=20 -pause=6` Displays the last twenty records from the system log, six records at a time

To add a remote target, see "add log-target (on page 37)."

uplinkport

Manage interconnect module uplink ports.

Supported actions: `add, help, remove, set, show`

Item	Description
`add uplinkport`	Add a new uplink port to an existing network or a shared uplink port set.
Syntax	`add uplinkport <PortID> [Network=<NetworkName> | UplinkSet=<UplinkSetName>] [Speed=<Auto|10Mb|100Mb|1Gb|10Gb|Disabled>] [Role=<Primary|Secondary>]`
Parameter	
`PortID (required)`	The ID of an uplink port to add. The ID is a combination of the enclosure name, interconnect bay, and port number in a single descriptor. The format of the port ID is "`<EnclosureID>:<InterconnectBay>:<PortNumber>`".
Properties	
`Network (required)`	The name of an existing network to which the port is added if the uplink set name has not been specified.
`UplinkSet (required)`	The name of an existing shared uplink port set to which the port is added if the network name has not been specified.
`Speed (optional)`	Specifies the port speed for the port (optional). Valid values include "Auto", "10Mb", "100Mb", "1Gb", "10Gb", and "Disabled". If not specified, the default

Item	Description
	port speed is "Auto". If there is no connector present on the uplink port, only "Auto" and "Disabled" can be configured as a possible speed. Speed restrictions apply.
`Role (optional)`	The role played by the port if the connection mode of the network or shared uplink set is selected as "Failover". The default is "Primary".
Examples	
	`->add uplinkport enc0:1:1 Network=MyNetwork` Adds a new uplink port (Bay 1, Port 1) to a network
	`->add uplinkport enc0:2:4 Network=MyNetwork Speed=1Gb` Adds a new uplink port (Bay 2, Port 4) to a network and sets the port speed
	`->add uplinkport enc0:2:3 UplinkSet=MyUplinkSet` Adds a new uplink port (Bay 2, Port 3) to a shared uplink port set
	`->add uplinkport enc0:2:4 Network=MyNetwork Role=Primary` Adds a new uplink port to a network with the connection mode as Failover and the port role as Primary

Item	Description
`remove uplinkport`	Remove an uplink port element from a network or a shared uplink port set.
Syntax	`remove uplinkport <PortID> [Network=<NetworkName> | UplinkSet=<UplinkSetName>]`
Parameters	
`PortID (required)`	The ID of the port to remove from a network. The port ID must be in the format `<EnclosureID>:<InterconnectBayNumber>:<PortNumber>` If EnclosureID is not specified, it defaults to the local enclosure.
`Network (optional)`	The name of the network from which the port is to be removed
`UplinkSet (optional)`	The name of the shared uplink port set from which the port is to be removed
Examples	
	`->remove uplinkport enc0:1:2 Network=MyNetwork` Removes a specific uplink port (Bay 1, Port 2) from a network
	`->remove uplinkport * Network=BlueNetwork` Removes all uplink ports from a network named "BlueNetwork"
	`->remove uplinkport enc0:2:3 UplinkSet=SharedUplinkSet1` Removes a specific uplink port (Bay 2, Port 3) from a shared uplink set

Item	Description
`set uplinkport`	Modify an uplink port that exists as a member of a network or shared uplink port set.
Syntax	`set uplinkport <PortID> [Network=<NetworkName> | UplinkSet=<UplinkSetName>][Speed=<Auto|10Mb|100Mb|1Gb|10Gb|Disabled>] [Role=<Primary|Secondary>]`
Parameter	
`PortID (required)`	The ID of the port to modify. The specified port must already be added to a network or uplink port set. The port ID is in the format

Item	Description
	<EnclosureID>:<BayNumber>:<PortNumber>
Properties	
Network (required)	The name of the network to which the port belongs if the uplink set name is not specified.
UplinkSet (required)	The name of the shared uplink port set to which the port belongs if the network name is not specified.
Speed (optional)	Specifies the port speed for the port. Acceptable values include "Auto", "10Mb", "100Mb", "1Gb", "10Gb", and "Disabled". If there is no connector present on the uplink port, only "Auto" and "Disabled" can be configured as possible speeds. Speed restrictions apply.
Role (optional)	The role played by the port if the connection mode of the network or shared uplink set is selected as "Failover". The default value is "Primary".
Examples	
	->set uplinkport enc0:1:2 Network=MyNetwork Speed=1Gb Changes the port speed of a network port
	->set uplinkport enc0:2:1 Network=MyNetwork Speed=Disabled Disables a specific port that belongs to a network
	->set uplinkport enc0:2:4 UplinkSet=MyUplinkSet Speed=Disabled Disables a specific port that belongs to a shared uplink set
	->set uplinkport enc0:2:4 Network=MyNetwork Role=Secondary Modifies the role of the network uplink port with the connection mode on the network or the shared uplink set as "Failover" to take the primary port role

Item	Description
show uplinkport	Display all Ethernet module uplink ports known to the domain. If the port is a member of a network or a shared uplink port set, then it appears also.
Syntax	show uplinkport <PortID | *> [FilterBy]
Parameters	
PortID (optional)	The ID of an uplink port. The PortID format is <EnclosureID>:<Bay>:<PortNumber>. "*" displays a detailed view of all uplink ports.
FilterBy (optional)	Filters the output of the show command by the specified attribute. The option is specified in the format <columnID>=<value>. For example, to display uplink ports belonging to enclosure enc0, the option would be specified as ID=enc0. To display all the ports using connector type RJ-45, the option would be Type=RJ45. You can specify more than one filter option for a single command; for example, show uplinkport ID=enc0 Type=RJ45.
Examples	
	->show uplinkport Displays all uplink ports
	->show uplinkport enc0:5:6 Displays details of uplink port 6 in bay 5 of the local enclosure
	->show uplinkport * Displays all uplink ports in the enclosure (detailed view)

Item	Description
	->show uplinkport ID=enc0:1 Displays all the uplink ports for the specific bay (for example, for bay 1)
	->show uplinkport status=Linked Displays all the uplink ports that are linked
	->show uplinkport ID=enc0:1 type=RJ45 Displays all the uplink ports for the specific bay 1 with connector type RJ-45

uplinkset

Manage shared uplink port sets

Supported actions: add, help, remove, set, show

Item	Description
add uplinkset	Create a new shared uplink port set.
Syntax	add uplinkset <UplinkSetName> [ConnectionMode=<Auto|Failover>]
Parameter	
UplinkSetName (required)	The unique name of the new shared uplink port set to create
Property	
ConnectionMode (optional)	Specifies the connection type that is formed when multiple ports are added to the uplinkset. Valid values include "Auto" and "Failover". The default value is "Auto".
Examples	
	->add uplinkset MyNewUplinkSet Creates a new shared uplink port set and adds it to the domain
	->add uplinkset MyNewUplinkSet ConnectionMode=Failover Creates a new shared uplinkset and sets the connection mode to failover

Item	Description
remove uplinkset	Remove a shared uplink port set from the domain.
Syntax	remove uplinkset <UplinkSetName | *>
Parameter	
UplinkSetName (required)	The name of an existing shared uplink port set. "*" removes all the existing uplink port sets from the domain.
Example	
	->remove uplinkset MyUplinkSet Removes a shared uplink port set

Item	Description
set uplinkset	Modify an existing shared uplink port set.
Syntax	set uplinkset <UplinkSetName> [Name=<NewName>] [ConnectionMode=<Auto|Failover>]
Parameter	

Item	Description
`UplinkSetName (required)`	The name of an existing shared uplink set to modify
Properties	
`Name (optional)`	The new name of the shared uplink set
`ConnectionMode (optional)`	Specifies the connection type that is formed when multiple ports are added to the uplinkset. Valid values include "Auto" and "Failover". The default value is "Auto".
Examples	
	`->set uplinkset Blue Name=Red` Changes the name of an shared uplink set from "Blue" to "Red"
	`->set uplinkset Blue connectionMode=Failover` Changes the connection mode of the uplink set

Item	Description
`show uplinkset`	Display shared uplink configurations.
Syntax	`show uplinkset [<UplinkSetName> | *]`
Parameter	
`UplinkSetName (optional)`	Name of an existing uplink port set. "*" displays a detailed view of all the uplink port sets. If not specified, summary of all uplink port sets will be displayed.
Examples	
	`->show uplinkset` Displays a summary listing of all uplink sets
	`->show uplinkset *` Displays detailed information for all shared uplink sets
	`->show uplinkset MyNetwork` Displays detailed information for a specific shared uplink set

user

Manage local domain user configurations.

Supported actions: `add, help, remove, set, show`

Item	Description
`add user`	Create a new user and add it to the Virtual Connect Manager database.
Syntax	`add user <UserName> Password=<password> [FullName=<Full Name>] [ContactInfo=<Contact Details>] [Enabled=<True|False>] [Privileges=<Storage|Network|Server|Domain|*>]`
Parameter	
`UserName (required)`	The name of the new user to add. The username must be unique within the domain.
Properties	

Item	Description
`Password (required)`	The password of the new user. The password of the new user can be entered as clear text in the command or as a masked string at the prompt.
`FullName (optional)`	The full name of the user
`ContactInfo (optional)`	Contact information for the user
`Enabled (optional)`	Enables or disables the user. Valid values include "true" and "false". If not specified, then the new user is enabled by default.
`Privileges (optional)`	The allowed privileges for the user. The privileges may be any combination of "domain", "server", "network", or "storage" separated by commas. If no privilege is specified, then the user has no privileges and can display domain information only. If "*" is specified, then all privileges apply.
Examples	
	`->add user steve Password=fgY87hHl` Adds a new user by specifying the minimal amount of properties
	`->add user bill Password=HGtwf7272562 Privileges="domain,network" FullName="Bill Johnson" ContactInfo=billj@company.com Enabled=true` Adds a new user and configures additional user properties
	`->add user Admin Password=hjkhfd Privileges=*` Adds an "Admin" user with all privileges

Item	Description
`remove user`	Remove a user from the Virtual Connect Manager database.
Syntax	`remove user <username | *>`
Parameter	
`UserName (required)`	The name of an existing user that will be removed. If "*" is specified, then all users except for the default Administrator account are removed.
Examples	
	`->remove user steve` Removes a specific user by name
	`->remove user *` Removes all users

Item	Description
`set user`	Modify attributes of an existing user.
Syntax	`set user <UserName> [<password>] [FullName=<Full Name>] [ContactInfo=<Contact Details>] [Enabled=<True|False>] [Privileges=<Storage|Network|Server|Domain|*>]`
Parameter	
`UserName (required)`	The name of the user to be modified
Properties	
`Password (optional)`	The new password of the user can be entered as clear text in the command or as a masked string at the prompt. If the Password value is blank, the user is prompted to enter the password at the prompt.

Item	Description
`FullName (optional)`	The full name of the user
`ContactInfo (optional)`	Contact information for the user
`Enabled (optional)`	Enables or disables the user. Valid values include "true" and "false".
`Privileges (optional)`	The allowed privileges for the user. Privileges can be any combination of "domain", "server", "network", "storage" separated by commas. If the privilege is blank, then the user has no privileges and can display domain information only. If "*" is specified, then all privileges apply.
Examples	
	`->set user steve Password=fgY87hHl` Modifies an existing user password
	`->set user steve Password` Modifies an existing user password, masked, at the prompt
	`->set user bill Password=HGtwf7272562 Privileges="domain,network" FullName="Bill Johnson" ContactInfo=billj@company.com Enabled=true` Modifies several properties of an existing user
	`->set user tom privileges=*` Gives a user all privileges

Item	Description
`show user`	Display user summary or user details.
Syntax	`show user [<username|*>]`
Parameter	
`UserName (optional)`	Name of an existing user in the VC domain. If not specified, then summary of all existing user will be displayed.
Examples	
	`->show user` Lists all existing users
	`->show user steve` Displays details of an existing user by name
	`->show user *` Displays details of all existing users

user-security

Manage local user security settings.

Supported actions: `help, set, show`

Item	Description
`set user-security`	Modify domain user security settings and enforce additional security requirements for user passwords.
Syntax	`set user-security [StrongPasswords=<Enabled|Disabled>] [MinPasswordLength=<3-40>]`
Properties	

Item	Description
`StrongPasswords (optional)`	Enables or disables strong password enforcement. If enabled, then new, local users that are created are validated against the password characteristics specified. Valid values include: "Enabled" and "Disabled".
`MinPasswordLength (optional)`	The minimum password length allowed for new passwords when adding a new user and when changing an existing password. The default value is 3.
Examples	
	`->set user-security StrongPasswords=Enabled` Enables strong user password enforcement
	`->set user-security StrongPasswords=Disabled` Disables strong user password enforcement
	`->set user-security MinPasswordLength=10` Modifies the minimum password length

Item	Description
`show user-security`	Display general domain user security settings.
Syntax	`show user-security`
Example	
	`->show user-security` Displays user security settings

vcm

Reset the Virtual Connect Manager.

Supported actions: `help, reset`

Item	Description
`reset vcm`	Reset the Virtual Connect Manager. A failover to the standby VCM may also be specified (optional), if there is a standby VCM available. **IMPORTANT:** Resetting the VCM causes a temporary loss in connectivity with the Virtual Connect Manager. If failover is specified and there is a standby VCM, users are logged off and must reconnect using the standby VCM IP address.
Syntax	`reset vcm [-failover]`
Option	
`Failover`	Forces a failover from the current primary Virtual Connect Manager to the standby manager
Examples	
	`->reset vcm` Resets the Virtual Connect Manager
	`->reset vcm -failover` Resets the Virtual Connect Manager and forces a failover to the standby VCM (if available)

version

Display CLI version information.

Supported actions: `help, show`

Item	Description
`show version`	Display CLI version information.
Syntax	`show version`
Example	`->show version` Displays CLI version and copyright information

Help subsystem

The help subsystem consists of three options:

- **Help summary**—lists all supported actions and a short description of each:

```
>help (or ?)
add          add an element to an existing object
assign       assign a server profile to a device bay
. . .
```

- **Subcommand help**—displays help details associated with a specific subcommand, including supported managed elements:

```
>assign -help (or assign ?)
assign a server profile to a device bay

Managed Elements:
profile

Examples:
assign profile MyProfile enc0:1
```

- **Management element help**—provides a listing of objects that are supported with a specific subcommand and a brief description of the management element and what it represents in the management model:

```
->help devicebay

General Enclosure Device Bay settings and information

Supported Subcommands:
help
show

------------------------------------------------------------------------

->show devicebay -help

Description:
```

```
  This command displays all device bays in the domain

Syntax:

  show devicebay [<DeviceBayName> | *]

Parameters:

  DeviceBayName : The reference name of a device bay in the domain.
                  The format of the device bay name is
                <EnclosureID:DeviceBay>

Examples:

  - Display a summary listing of all device bays:
    ->show devicebay

  - Show detailed information for all device bays:
    ->show device bay *

  - Show detailed information for a specific device bay 2 of
    a specific enclosure:
    ->show devicebay enc0:2
```

Output format

The CLI provides two different output formats:

- Interactive user output format
- Scriptable output format

The interactive user output format is the default. However, by using a command-line option, the user can also specify a "parse-friendly" output format, which provides data in a format that can be easily interpreted by automated scripts invoking the CLI. The different output formats primarily impact the `show` subcommand in the CLI infrastructure, where a majority of the informational details are displayed.

Interactive user output format

The interactive user output format provides a user friendly view of information at the command line. When providing an overview, or listing, of several instances of data, a tabular text format is displayed. If an individual instance of data is being displayed, then the stanza format is used.

Example 1: Tabular text output format for displaying a user list

```
->show user
==============================================================================
UserName        Privileges FullName             ContactInfo          Enabled
==============================================================================
```

```
Administrator   domain     Steve Johnson        steve.johnson@hp.com true
                server
                network
                storage
-------------------------------------------------------------------------
Admin           domain     Admin                Admin                true
                server
                network
                storage
-------------------------------------------------------------------------
steve           domain     Steve Johnson        steve.johnson@hp.com true
                server
                network
                storage
-------------------------------------------------------------------------
brad            domain     Brad Mills           brad.mills@hp.com    true
                server
-------------------------------------------------------------------------
jim             network    Jimmy Joe            jimmy.joe@hp.com     true
-------------------------------------------------------------------------
alice           storage    Alice Candle         alice.candle@hp.com  false
-------------------------------------------------------------------------
```

Example 2: Stanza output format for displaying a single user instance

```
->show user steve
UserName    : steve
Privileges  : domain,server,network,storage
FullName    : Steve Johnson
ContactInfo : steve.johnson@hp.com
Enabled     : true
```

Example 3: Stanza output format for displaying all user details

```
->show user *
UserName    : Administrator
Privileges  : domain,server,network,storage
FullName    : Steve Johnson
ContactInfo : steve.johnson@hp.com
Enabled     : true

UserName    : Admin
Privileges  : domain,server,network,storage
FullName    : Admin
ContactInfo : Admin
Enabled     : true
```

```
UserName    : steve
Privileges  : domain,server,network,storage
FullName    : Steve Johnson
ContactInfo : steve.johnson@hp.com
Enabled     : true

UserName    : brad
Privileges  : domain,server
FullName    : Brad Mills
ContactInfo : brad.mills@hp.com
Enabled     : true

UserName    : jim
Privileges  : network
FullName    : Jimmy Joe
ContactInfo : jimmy.joe@hp.com
Enabled     : true

UserName    : alice
Privileges  : storage
FullName    : Alice Candle
ContactInfo : alice.candle@hp.com
Enabled     : false
```

Scriptable output format

Scriptable output format allows scripts to invoke CLI commands and receive command responses that can be easily parsed by the scripts. This capability is provided by two options that are available: -output=script1 and -output=script2. These options are described in more detail below. To display output with no headers or labels, use no-headers as an additional output option value.

IMPORTANT: If the delimiter is present within the data, then the entire value is surrounded by double quotes.

- **Script1 Output Format**

  The script1 output format can be used to format the output using a name-value pair format, using an equal sign as the delimiter. All text on the left side of the equal sign designates the "name" of a property, and the text on the right side of the equal sign designates the "value" of the property. If "no-headers" is provided as an additional option value, only the values are displayed. Each property is displayed on a separate line.

- **Script2 Output Format**

  The script2 output format can be used to format all instance data in a single line, using a semi-colon as the delimiter for the data. The first line contains the property names. This format is consistent with a "table view" of the data, where the first line is represented by a list of column labels, while the remaining lines provide the actual data being displayed. Each line represents a single instance of data. For example, in the case of showing users, each line provides all data corresponding to a single user instance.

The following examples provide some common scenarios for using the script output format options.

Example 1: Scriptable output format displaying all enclosures

```
->show enclosure -output=script1
ID=enc0
Name=Enclosure1
Import Status=Imported
Serial Number=USE0000BK2
Part Number=403321-021
Asset Tag=OA ASSET 453
```

Example 2: Scriptable output format displaying user "Administrator" information

```
->show user Administrator -output=script1
User Name=Administrator
Privileges=domain,server,network,storage
Full Name=
Contact Info=
Enabled=true
```

Example 3: Scriptable output format displaying all users (with table header)

```
->show user -output=script2
UserName;Privileges;FullName;ContactInfo;Enabled
Administrator;domain,server,network,storage;Steve
Johnson;steve.johnson@hp.com;true
Admin;domain,server,network,storage;Admin;Admin;true
steve;domain,server,network,storage;Steve
Johnson;steve.johnson@hp.com;true
```

Example 4: Scriptable output format displaying all users (no table header)

```
->show user -output=script2,no-headers
Administrator;domain,server,network,storage;Steve
Johnson;steve.johnson@hp.com;true
Admin;domain,server,network,storage;Admin;Admin;true
steve;domain,server,network,storage;Steve
Johnson;steve.johnson@hp.com;true
```

Example 5: Scriptable output format displaying a single user (with table header)

```
->show user steve -output=script2
UserName;Privileges;FullName;ContactInfo;Enabled
steve;domain,server,network,storage;Steve
Johnson;steve.johnson@hp.com;true
```

Example 6: Scriptable output format displaying a single user (no table header)

```
->show user steve -output=script2,no-headers
steve;domain,server,network,storage;Steve
Johnson;steve.johnson@hp.com;true
```

Statistics descriptions

Ethernet modules

Ethernet uplink and downlink ports

Name	RFC	Description
rfc1213_IfInDiscards	1213	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
rfc1213_IfInErrors	1213	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
rfc1213_IfInNUcastPkts	1213	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
rfc1213_IfInOctets	1213	The total number of octets received on the interface, including framing characters.
rfc1213_IInUcastPkts	1213	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
rfc1213_IfInUnknownProtos	1213	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
rfc1213_IfOutDiscards	1213	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
rfc1213_IOutErrors	1213	The number of outbound packets that could not be transmitted because of errors.
rfc1213_IfOutNUcastPkts	1213	The total number of packets that higher-level protocols requested

Name	RFC	Description
		be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
rfc1213_IfOutOctets	1213	The total number of octets transmitted out of the interface, including framing characters.
rfc1213_IfOutQLen	1213	The length of the output packet queue (in packets).
rfc1213_IfOutUcastPkts	1213	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
rfc1213_IpForwDatagrams	1213	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this ounter will include only those packets which were ource-Routed via this entity, and the Source-Route option processing was successful.
rfc1213_IpInDiscards	1213	The number of input IP datagrams for which no problems were encountered to prevent their ontinued processing, but which were discarded e.g., for lack of buffer space). Note that this ounter does not include any datagrams discarded hile awaiting re-assembly.
rfc1213_IpInHdrErrors	1213	The number of input datagrams discarded due to rrors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered n processing their IP options, etc.
rfc1213_IpInReceives	1213	The total number of input datagrams received from interfaces, including those received in error.
rfc1493_Dot1dBasePortDelayExceededDiscards	1493	The number of frames discarded by this port due to excessive transit delay through the bridge. It i incremented by both transparent and source route bridges.
rfc1213_Dot1dBasePortMtu	1493	The number of frames discarded

Name	RFC	Description
ExceededDiscards		by this port due to an excessive size. It is incremented by both transparent and source route bridges.
rfc1213_Dot1dPortInDiscards	1493	Count of valid frames received which were discarded (i.e., filtered) by the Forwarding Process.
rfc1213_Dot1dTpPortInFrames	1493	The number of frames that have been received by his port from its segment. Note that a frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
rfc1757_StatsBroadcastPkts	1757	The number of good packets received during this sampling interval that were directed to the broadcast address
rfc1757_StatsCRCAlignErrors	1757	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rfc1757_StatsCollisions	1757	The best estimate of the total number of collisions n this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10BASE-5) and section 10.3.1.3 (10BASE-2) of IEEE standard 802.3 states that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment would.

Name	RFC	Description
		Probe location plays a much smaller role when considering 10BASE-T. 14.2.1.4 (10BASE-T) of IEEE standard 802.3 defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BASE-T station can only detect collisions when it is transmitting. Thus probes placed on a station and a repeater, should report the same number of collisions. Note also that an RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
rfc1757_StatsDropEvents	1757	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
rfc1757_StatsFragments	1757	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that it is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
rfc1757_StatsJabbers	1757	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-

Name	RFC	Description
		integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
rfc1757_StatsMulticastPkts	1757	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
rfc1757_StatsOctets	1757	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The differences in the sampled values are Pkts and Octets, respectively, and the number of seconds in the interval is Interval. These values are used to calculate the Utilization as follows: Pkts * (9.6 + 6.4) + (Octets * .8) Utilization = ---------- Interval * 10,000 The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent."
rfc1757_StatsOversizePkts	1757	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
rfc1757_StatsPkts	1757	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Name	RFC	Description
rfc1757_StatsPkts1024to1518Octets	1757	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
rfc1757_StatsPkts128to255Octets	1757	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
rfc1757_StatsPkts256to511Octets	1757	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
rfc1757_StatsPkts512to1023Octets	1757	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
rfc1757_StatsPkts64Octets	1757	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
rfc1757_StatsPkts65to127Octets	1757	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
rfc1757_StatsTXNoErrors	1757	All packets transmitted without error, less oversized packets.
rfc1757_StatsUndersizePkts	1757	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
rfc2233_IfHCInBroadcastPkts	2233	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts. Discontinuities in the value of this counter can occur at re-

Name	RFC	Description
		initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCInMulticastPkts	2233	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifInMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCInOctets	2233	The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCOutUcastPkts	2233	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCOutBroadcastPckts	2233	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the

Name	RFC	Description
		management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCOutMulticastPkts	2233	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifOutMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCOutOctets	2233	The total number of octets transmitted out of the interface, including framing characters. This object is a 64-bit version of ifOutOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCOutUcastPkts	2233	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3ControlInUnknownOpcodes	2665	A count of MAC Control frames received on this interface that contain an opcode that is not supported by this device. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Name	RFC	Description
rfc2665_Dot3InPauseFrames	2665	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3OutPauseFrames	2665	A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsAlignmentErrors	2665	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. This counter does not increment for 8-bit wide group encoding schemes. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsCarrierSenseErrors	2665	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented

Name	RFC	Description
		by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsDeferredTransmissions	2665	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsExcessiveCollisions	2665	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsFCSErrors	2665	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions

Name	RFC	Description
		obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. Note: Coding errors detected by the physical layer for speeds above 10 Mb/s will cause the frame to fail the FCS check. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsFrameTooLongs	2665	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsInternalMacReceiveErrors	2665	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of

Name	RFC	Description
		receive errors on a particular interface that are not otherwise counted. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsInternalMacTransmitErrors	2665	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsLateCollisions	2665	The number of times that a collision is detected on a particular interface later than one slotTime into the transmission of a packet.A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsSQETTest	2665	dot3StatsSQETestErrors - A count

Name	RFC	Description
Errors		of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 1998 Edition, section 7.2.4.6. This counter does not increment on interfaces operating at speeds greater than 10 Mb/s, or on interfaces operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsSingleCollisionFrames	2665	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsSymbolErrors	2665	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one

Name	RFC	Description
		occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

FCoE downlink ports

Name	RFC	Description
fcAddressErrors	4044	fcmPortAddressErrors - The number of frames received with unknown addressing; for example, an unknown SID or DID.
fcBBCreditFrameFailures	N/A	The number of times more frames were lost during a credit recovery period than the recovery process could resolve. This causes a Link Reset to recover the credits.
fcBBCreditRRDYFailures	N/A	The number of Buffer-to-Buffer Credit Recovery (BBCR) Receiver Ready (R_RDY) failures. This is the number of times more R_RDYs were lost during a credit recovery period than the recovery process could resolve. This causes a Link Reset to recover the credits.
fcClass2RxFrames	4044	fcmPortClass2RxFrames - The number of Class 2 frames received at this port.
fcClass2TxFrames	4044	fcmPortClass2TxFrames - The number

Name	RFC	Description
		of Class 2 frames transmitted out of this port.
fcClass3Discards	4044	fcmPortClass3Discards - The number of Class 3 frames that were discarded upon reception at this port.
fcClass3RxFrames	4044	fcmPortClass3RxFrames - The number of Class 3 frames received at this port.
fcClass3TxFrames	4044	fcmPortClass3TxFrames - The number of Class 3 frames transmitted out of this port.
fcDecodeErrors	N/A	The number of errors while converting the incoming 10-bit data stream into an 8-bit data for processing. Increasing value of this counter indicates potential hardware problem between module and FC mezzanine serdes settings.
fcFBSYFrames	4044	fcmPortClass2RxFbsyFrames - The number of times that F_BSY was returned to this port as a result of a Class 2 frame that could not be delivered to the other end of the link. This can occur when either the fabric or the destination port is temporarily busy. Note that this counter will never increment for an F_Port.
fcFRJTFrames	4044	fcmPortClass2RxFrjtFrames - The number of times that F_RJT was returned to this port as a result of a Class 2 frame that was rejected by the fabric. Note that this counter will never increment for an F_Port.
fcFramesTooLong	4044	fcmPortFrameTooLongs - The number of frames received at this port for which the frame length was greater than what was agreed to in FLOGI/PLOGI. This could be caused by losing the end of frame delimiter
fcFramesTruncated	4044	fcmPortTruncatedFrames - The number of frames received at this port for which the frame length was less than the minimum indicated by the frame header - normally 24 bytes, but it could be more if the DFCTL field indicates an optional header should have been present.
fcInvalidCRC	4044	fcmPortInvalidCRCs - The number of frames received with an invalid CRC. This count is part of FC-PH's Link

Name	RFC	Description
		Error Status Block (LESB).
fcInvalidTxWords	4044	fcmPortInvalidTxWords - The number of invalid transmission words received at this port. This count is part of FC-PH's Link Error Status Block (LESB).
fcLinkFailures	4044	fcmPortLinkFailures - The number of link failures. This count is part of FC-PH's Link Error Status Block (LESB).
fcLossOfSynchronization	4044	fcmPortLossofSynchs - The number of instances of synchronization loss detected at this port. This count is part of FC-PH's Link Error Status Block (LESB).
fcNumberLinkResets	4044	fcmPortLinkResets - The number of times the reset link protocol was initiated on this port. This includes the number of Loop Initialization Primitive (LIP) events on an arbitrated loop port.
fcNumberOfflineSequences	FCMGMT-MIB	connUnitPortStatCountNumberOfflineSequences - Count of Offline Primitive sequence received at this port. Note, this is a Fibre Channel only stat.
fcPrimitiveSeqProtocolErrors	4044	fcmPortPrimSeqProtocolErrors - The number of primitive sequence protocol errors detected at this port. This count is part of FC-PH's Link Error Status Block (LESB).
fcRxByteRate	N/A	Average receive byte rate (Byte/s) for sample period of once a second.
fcRxFrameRate	N/A	Average receive frame rate (frame/s) for sample period of once a second.
fcRxLinkResets	4044	fcmPortRxLinkResets - The number of Link Reset (LR) Primitive Sequences received.
fcRxOfflineSequences	4044	fcmPortRxOfflineSequences - The number of Offline (OLS) Primitive Sequences received at this port.
fcSmoothingOverflowErrors	N/A	The number of times that a violation of FC rules on the incoming signal were detected. An example of a violation would be an insufficient number of idles were received between the frames.
fcTotalRxBytes	N/A	Total number of bytes received.

Name	RFC	Description
fcTotalRxFrames	N/A	Total number of frames received.
fcTotalTxBytes	N/A	Total number of bytes transmitted.
fcTotalTxFrames	N/A	Total number of frames transmitted.
fcTxByteRate	N/A	Average transmit byte rate (Byte/s) for sample period of once a second.
fcTxFrameRate	N/A	Average transmit frame rate (frame/s) for sample period of once a second.
fcTxLinkResets	4044	fcmPortTxLinkResets - The number of Link Reset (LR) Primitive Sequences transmitted.
fcTxOfflineSequences	4044	fcmPortTxOfflineSequences - The number of Offline (OLS) Primitive Sequences transmitted by this port.

Fibre channel ports

FC uplink ports

Name	RFC	Description
numAddressErrors	FCMGMT-MIB	connUnitPortStatCountAddressErrors - Count of frames received with unknown addressing. e.x. unknown SID or DID. the SID or DID is not known to the routing algorithm.
numBBCreditZero	FCMGMT-MIB	connUnitPortStatCountBBCreditZero - Count of transitions in/out of BBcredit zero state. The other side is not providing any credit.
numBytesRx	N/A	Total number of bytes received.
numBytesTx	N/A	Total number of bytes transmitted.
numCRCErrors	FCMGMT-MIB	connUnitPortStatCountInvalidCRC - Count of frames received with invalid CRC. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Loop ports should not count CRC errors passing through when monitoring.
numClass3Discards	FCMGMT-MIB	connUnitPortStatCountClass3Discards - Count of Class 3 Frames that were discarded upon reception at this port. There is no FBSY or FRJT generated for Class 3 Frames. They are simply discarded if they cannot be delivered.
numEncodingDisparityErrors	FCMGMT-MIB	connUnitPortStatCountEncodingDisparityErrors - Count of disparity errors received at this port.

Name	RFC	Description
numFBSYFrames	FCMGMT-MIB	connUnitPortStatCountFBSYFrames - Count of times that FBSY was returned to this port as a result of a frame that could not be delivered to the otherend of the link. This occurs if either the Fabric or the destination port is temporarily busy. Port can only occur on SOFc1 frames (the frames that establish a connection). This is the sum of all classes.
numFRJTFrames	FCMGMT-MIB	connUnitPortStatCountFRJTFrames - Count of times that FRJT was returned to this port as a result of a Frame that was rejected by the fabric. Note, This is the total for all classes.
numFramesTooLong	FCMGMT-MIB	connUnitPortStatCountFramesTooLong - Count of frames received at this port where the frame length was greater than what was agreed to in FLOGI/PLOGI. This could be caused by losing the end of frame delimiter.
numInputBuffersFull	FCMGMT-MIB	connUnitPortStatCountInputBuffersFull - Count of occurrences when all input buffers of a port were full and outbound buffer-to-buffer credit transitioned to zero. There is no credit to provide to other side.
numInvalidOrderedSets	FCMGMT-MIB	connUnitPortStatCountInvalidOrderedSets - Count of invalid ordered sets received at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8).
numInvalidTransmissionWords	FCMGMT-MIB	connUnitPortStatCountInvalidTxWords - Count of invalid transmission words received at this port. This count is part of the Link Error Status Block (LESB).
numLRsRx	FCMGMT-MIB	connUnitPortStatCountRxLinkResets - Count of Link resets. This is the number of LRs received. Note, this is a Fibre Channel only stat.
numLRsTx	FCMGMT-MIB	connUnitPortStatCountTxLinkResets - Count of Link resets. This is the number LRs transmitted.
numLinkFailures	FCMGMT-MIB	connUnitPortStatCountLinkFailures - Count of link failures. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8).
numLossOfSignal	FCMGMT-MIB	connUnitPortStatCountLossofSignal - Count of instances of signal loss detected at port. This count is part of the Link Error Status Block (LESB). (FC-

Name	RFC	Description
		PH 29.8).
numLossOfSync	FCMGMT-MIB	connUnitPortStatCountLossofSynchronization - Count of instances of synchronization loss detected at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note
numMcastFramesRx	FCMGMT-MIB	connUnitPortStatCountRxMulticastObjects - Count of Multicast Frames or Packets received at this port.
numMcastFramesTx	FCMGMT-MIB	connUnitPortStatCountTxMulticastObjects - Count of Multicast Frames or Packets transmitted out this port.
numMcastTimeouts	N/A	Number of timeouts reported for multicast frames. A single frame could cause this counter to increment if it timed out for each multiple destination.
numPrimitiveSeqProtocolErr	FCMGMT-MIB	connUnitPortStatCountPrimitiveSequenceProtocolErrors - Count of primitive sequence protocol errors detected at this port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8).
numRxBadEOFs	N/A	The number of frames received with a badly formed end-of-frame.
numRxCRCs	N/A	Received frames: the number of CRC errors detected.
numRxClass1Frames	FCMGMT-MIB	connUnitPortStatCountClass1RxFrames - Count of Class 1 Frames received at this port. Note, this is a Fibre Channel only stat.
numRxClass2Frames	FCMGMT-MIB	connUnitPortStatCountClass2RxFrames - Count of Class 2 Frames received at this port
numRxClass3Frames	FCMGMT-MIB	connUnitPortStatCountClass3RxFrames - Count of Class 3 Frames received at this port.
numRxLCs	N/A	Number of link control frames received at this port
numRxOfflineSequences	FCMGMT-MIB	connUnitPortStatCountRxOfflineSequences - Count of Offline Primitive OLS received at this port.
rxBytePeakRate	N/A	Receive max byte rate since last reset - (bytes/sec)
rxByteRate	N/A	Receive instantaneous byte rate - (bytes/sec)
rxFramePeakRate	N/A	Receive max frame rate since last reset

Name	RFC	Description
		– (frames/sec)
rxFrameRate	N/A	Receive instantaneous frame rate - (frames/sec)
samplingRate	N/A	This controls the rate of statistics sampling in switch ports. Polling must be frequent enough to avoid counter overflow for errors and tx/rx bytes
sfpStatus	N/A	SFP status.
txBytePeakRate	N/A	Transmission max byte rate since last reset - (bytes/sec)
txByteRate	N/A	Receive instantaneous byte rate - (bytes/sec)
txFramePeakRate	N/A	Transmission max frame rate since last reset - (frames/sec)
txFrameRate	N/A	Transmission instantaneous frame rate - (frames/sec)

Downlink ports

Statistics are not currently available for downlink fibre channel ports.

Configuring the Virtual Connect domain using the CLI

Basic configuration

A Virtual Connect domain consists of an enclosure and a set of associated modules and server blades that are managed together by a single instance of the Virtual Connect Manager. The Virtual Connect domain contains specified networks, server profiles, and user accounts that simplify the setup and administration of server connections. Establishing a Virtual Connect domain enables administrators to upgrade, replace, or move servers within their enclosures without changes being visible to the external LAN/SAN environments.

Before starting, perform the following tasks:

- Verify that the HP Onboard Administrator is running the latest firmware (must be at least v2.20 or later).
- Locate the Default Network Settings label attached to the Ethernet module in bay 1 of the primary enclosures and note the following information:
  - DNS name
  - User name
  - Password
- Connect any Ethernet module stacking cables

IMPORTANT: After a CLI command is issued, it can take up to 90 seconds before configuration changes are stored in persistent memory. Disruptive actions such as powering cycling an I/O module within this time window can result in lost configuration changes.

The following sections provide the necessary steps to set up a basic domain.

For detailed information on a particular command, see "Managed elements (on page 13)."

Logging in to the CLI

The Virtual Connect Manager CLI can be accessed remotely through any SSH session ("Remote access to the Virtual Connect Manager" on page 11):

- SSH

```
>ssh 192.168.0.120
login as: Administrator
password:
```

- Local User Authentication using default Administrator login credentials

```
>ssh 192.168.0.120
login as: Administrator
password: <Default Administrator login credentials>
```

- LDAP Authentication

```
>ssh 192.168.0.120
login as: <LDAP user>
password: <password>
```

Domain setup

A Virtual Connect domain consists of an enclosure and a set of associated modules and server blades that are managed together by a single instance of the Virtual Connect Manager. the Virtual Connect domain contains specified networks, server profiles, and user accounts that simplify the setup and administration of server connections. Establishing a Virtual Connect domain enables administrators to upgrade, replace, or move servers within their enclosures without changes being visible to the external LAN/SAN environments.

Before starting, perform the following tasks:

- Verify that the Onboard Administrator is running the latest firmware.
- Locate the Default Network Settings label attached to the Ethernet module in bay 1 of the primary enclosure and note the following information:
  - DNS name
  - User name
  - Password
- Connect any Ethernet module stacking cables

After logging in, perform the following tasks to set up the domain:

1. Import the enclosure.
2. Name the domain.
3. Set up local user accounts and privileges.

Importing an enclosure

Enter OA credentials during import:

```
>import enclosure username=Administrator password=myPassword
```

or

```
>import enclosure username=Administrator
Password=*****
```

Setting the domain name

To set the domain name, use the `set domain` command:

```
>set domain name=MyNewDomainName
```

The Virtual Connect domain name must be unique within the data center, and can be up to 64 characters without spaces or special characters.

Configuring local users

- Add a new user

```
>add user bob password=fhkjdhfk privileges=domain,network
```

- Modify an existing user

  ```
  >set user bob fullname="Bob J Smith" enabled=false
  ```

- Remove an existing user

  ```
  >remove user bob
  ```

- Remove all local users except for the Administrator account

  ```
  >remove user *
  ```

Display local users:

- Summary display

  ```
  >show user
  ```

- Detailed display

  ```
  >show user *
  ```

- Display info on a single user

  ```
  >show user steve
  ```

Up to 32 local user accounts can be created.

Each account can be set up to have a combination of up to four access privileges:

- Domain
  - Define local user accounts, set passwords, define roles
  - Import enclosures
  - Name the VC domain
  - Set the domain IP address
  - Update firmware
  - Administer SSL certificates
  - Delete the VC domain
  - Save configuration to disk
  - Restore the configuration from a backup
  - Configure SNMP settings
- Networking
  - Configure network default settings
  - Select the MAC address range to be used by the VC domain
  - Create, delete, and edit networks
  - Create, delete, and edit shared uplink sets
  - Configure Ethernet SNMP settings
- Server
  - Create, delete, and edit server Virtual Connect profiles
  - Assign and unassign profiles to device bays
  - Select and use available networks
  - Select serial numbers (logical) and UUIDs (logical) to be used by server profiles
  - Power on and off server blades within the enclosure
- Storage

- Select the WWNs to be used by the domain
- Set up the connections to the external FC Fabrics
- Configure FC SNMP settings

It is possible to create a user with no privileges. This user can only view status and settings.

NOTE: The vcmuser_ account is an internal Onboard Administrator account created and used by Virtual Connect Manager to communicate with the Onboard Administrator. This account can show up in the Onboard Administrator system log. This account cannot be changed or deleted.

Configuring LDAP authentication support for users

- Set LDAP properties

  ```
  >set ldap serveraddress=192.168.0.110 enabled=true
  ```

- Add or Remove LDAP directory groups

  ```
  >add ldap-group MyNewGroup description="This is my test group"
  privileges=domain,server,network
  ```

- Enable or Disable local users

  ```
  >set ldap localusers=disabled
  ```

- Display LDAP settings and directory groups

  ```
  >show ldap
  >show ldap-group
  ```

Network setup

To establish external Ethernet network connectivity for the HP BladeSystem c-Class enclosure, do the following:

1. Identify the MAC addresses to be used on the server blades deployed within this Virtual Connect domain.
2. Setup connections from the HP BladeSystem c-Class enclosure to the external Ethernet networks.

   These connections can be uplinks dedicated to a specific Ethernet network or shared uplinks that carry multiple Ethernet networks with the use of VLAN tags.

Configuring MAC Address ranges

- Use VC-Defined MAC addresses

  ```
  >set domain MacType=VC-Defined MacPool=10
  ```

- Use factory-default MAC addresses

  ```
  >set domain MacType=Factory-Default
  ```

- Set user-defined MAC addresses

  ```
  >set domain MacType=User-Defined MacStart=00-17-A4-77-00-00 MacEnd=00-
  17-A4-77-00-FF
  ```

IMPORTANT: Configuring Virtual Connect to assign server blade MAC addresses requires careful planning to ensure that the configured range of MAC addresses is used once within the environment. Duplicate MAC addresses on an Ethernet network can result in a server network outage.

Each server blade Ethernet NIC ships with a factory default MAC address. The MAC address is a 48-bit number that uniquely identifies the Ethernet interface to other devices on the network. While the hardware ships with default MAC addresses, Virtual Connect has the ability to assign MAC addresses that will override the factory default MAC addresses while the server remains in that Virtual Connect enclosure. When configured to assign MAC addresses, Virtual Connect securely manages the MAC addresses by accessing the physical NICs through the enclosure Onboard Administrator and the iLO interfaces on the individual server blades.

Always establish control processes to ensure that a unique MAC address range is used in each Virtual Connect domain in the environment. Reusing address ranges could result in server network outages caused by multiple servers having the same MAC addresses.

If using Virtual Connect assigned MAC addresses, the following notes apply:

- Virtual Connect automatically reserves both a primary address and an iSCSI MAC address for use by multifunction gigabit server adapters, such as the HP NC373m PCI Express Dual Port Multifunction Gigabit server adapter. Only the primary MAC address is used by standard (not multifunction) Ethernet devices.
- If a server blade is moved from a Virtual Connect managed enclosure to a non-Virtual Connect enclosure, the local MAC addresses on that server blade are automatically returned to the original factory defaults.
- If a server blade is removed from a bay within a Virtual Connect domain and installed in another bay in the same Virtual Connect domain or in a bay in a different domain, it is assigned the new set of addresses appropriate for that server location.

Assigned MAC addresses

The MAC address range used by the Virtual connect domain must be unique within the environment. HP provides a set of pre-defined ranges that are for use by Virtual Connect Manager and will not conflict with server factory default MAC addresses.

When using the HP-defined MAC address ranges, ensure that each range is used only once within the environment.

Selecting VC-assigned MAC address ranges

When using VC-assigned MAC addresses, you can choose between using an HP pre-defined MAC address range or using a user-defined MAC address range.

- HP pre-defined MAC address range (recommended). These pre-defined ranges are reserved and appear as factory default on any hardware. There are 64 ranges of 1024 unique addresses to choose from. Be sure to use each range only once within a data center.
- User-defined MAC address range. To avoid potential conflict with other hardware MAC addresses in the environment, consider using a subrange of MAC addresses reserved by the IEEE for locally-administered MAC addresses. Ensure that the range does not conflict with any Ethernet device already deployed within the enterprise.

IMPORTANT: If you plan to use RDP for RedHat Linux installation and also plan to use User- or HP-defined MAC addresses, you must import the enclosure before running RDP.

NOTE: After any server profiles are deployed using a selected MAC address range, that range cannot be changed until all server profiles are deleted.

Creating an enet-network

To create a new Ethernet network use the `add network` command:

```
>add network MyNetworkName
```

Modifying enet-network properties

To modify Ethernet network properties, use the `set network` command:

```
>set network MyNetworkName state=enabled name=NewName smartlink=enabled
```

Displaying enet-networks

To display Ethernet network properties, use the `show network` command:

- Summary display

  ```
  >show network
  ```

- Detailed display

  ```
  >show network *
  ```

- Single network display

  ```
  > show network MyNetwork
  ```

Adding uplink ports to an enet-network

To add uplink ports to an existing Ethernet network, use the `add uplinkport` command:

```
>add uplinkport enc0:1:1 network=MyNetwork
```

Modifying uplink port properties

To modify an uplink port that exists as a member of a network or shared uplink set, use the `set uplinkport` command:

```
>set uplinkport network=Network1 speed=1Gb
```

Creating a shared uplink port set

To create a shared uplink port set, use the `add uplinkset` command:

```
>add uplinkset MyUplinkSetName
```

A shared uplink set is a way of identifying #*!<unassigned_variable!*# uplinks that will carry multiple networks over the same cable. In this case, each Ethernet packet carries a VLAN tag (IEEE 802.1Q) to identify the specific network to which it belongs. On shared uplinks, the VLAN tags are added when packets leave the VC-enabled enclosure and are removed when packets enter the enclosure. The external Ethernet switch and the Virtual Connect Manager must be configured to use the same VLAN tag identifier (a number between 1 and 4094) for each network on the shared uplink(s).

Virtual Connect places no special restrictions on which VLAN identifiers can be used, so the VLAN IDs already used for the networks in the data center can be used on these shared uplinks. To configure a shared uplink set for VLAN tagging, obtain a list of the network names and their VLAN IDs.

A shared uplink set enables multiple ports to be included to support port aggregation and link failover with a consistent set of VLAN tags.

Because VLAN tags are added or removed when Ethernet packets leave or enter the VC-Enet shared uplink, the VLAN tags have no relevance after the Ethernet packet enters the enclosure.

IMPORTANT: If you are deploying a server where VLAN tags will be used (added) on the server itself, do not connect the server Ethernet port carrying VLAN-tagged traffic to a shared uplink set.

Identifying an associated network as the native VLAN causes all untagged incoming Ethernet packets to be placed onto this network. Only one associated network can be designated as the native VLAN. All out-going Ethernet packets are VLAN tagged.

Displaying shared uplink port sets

- Summary display
  ```
  >show uplinkset
  ```
- Detailed display
  ```
  >show uplinkset *
  ```
- Single uplinkset display
  ```
  >show uplinkset MyUplinkSetName
  ```

Adding uplink ports to a shared uplink port set

To add uplink ports to a shared uplink port set, use the `add uplinkport` command:

```
>add uplinkport enc0:1:2 uplinkset=MyUplinkSetName
```

Creating a network that uses a shared uplink port set

To create a network that uses a shared uplink port set, use the `add network` command:

```
>add network MyNewNetworkName uplinkset=MyUplinkSetName vlanid=156
```

Server VLAN Tagging Support

With VC 1.31 and lower, each server port could be connected to a single virtual network. With v1.31 and higher, each server port can be connected to multiple virtual networks, each using a unique server VLAN ID for virtual network mapping.

This feature can be turned off or turned on by using the following command:

```
>set enet-vlan VLanTagControl=Tunnel
```

```
>set enet-vlan VlanTagControl=Map
```

If upgrading firmware to VC v1.31 or higher, this feature is disabled by default.

If Virtual Connect is set to map VLAN tags, the translation of Server VLAN tags to internal network VLAN and again to external data center VLAN tags, and the reverse, on incoming and outgoing frames can result in a configuration where the server VLANs might not match the external VLANs used on uplinks. To

avoid this scenario, the server connections can be forced to use the same VLAN mappings as the shared uplink sets.

```
>set enet-vlan VLanTagControl=Map SharedServerVLanId=true
```

When using mapped VLAN tags, the overall link speed can be controlled as follows:

```
> set enet-vlan PrefSpeedType=Custom PrefSpeed=500 MaxSpeedType=Custom
MaxSpeed=2500
```

Fibre Channel setup

To configure external Fibre Channel connectivity for the HP BladeSystem c-Class enclosure, do the following:

1. Identify WWNs to be used on the server blades deployed within this Virtual Connect Domain.
2. Define SAN fabrics.

Configuring WWN address ranges

- VC-Defined

  ```
  >set domain WwnType=VC-Defined WwnPool=5
  ```

- Factory-Default

  ```
  >set domain WwnType=Factory-Default
  ```

Each server blade FC HBA mezzanine card ships with factory default port and node WWNs for each FC HBA port. Each WWN is a 64-bit number that uniquely identifies the FC HBA port/node to other devices on the network. While the hardware ships with default WWNs, Virtual Connect has the ability to assign WWNs that will override the factory default WWNs while the server remains in that Virtual Connect enclosure. When configured to assign WWNs, Virtual Connect securely manages the WWNs by accessing the physical FC HBA through the enclosure Onboard Administrator and the iLO interfaces on the individual server blades.

When assigning WWNs to a FC HBA port, Virtual Connect will assign both a port WWN and a node WWN. Because the port WWN is typically used for configuring fabric zoning, it is the WWN displayed throughout the Virtual Connect user interface. The assigned node WWN is always the same as the port WWN incremented by one.

Configuring Virtual Connect to assign WWNs in server blades maintains a consistent storage identity (WWN) even when the underlying server hardware is changed. This method allows server blades to be replaced without affecting the external Fibre Channel SAN administration.

△ **CAUTION:** To avoid storage networking issues and potential loss of data associated with duplicate WWNs on a FC SAN fabric, plan carefully when allowing Virtual Connect to assign server blade WWNs so that the configured range of WWNs is used only once within the environment.

The WWN range used by the Virtual Connect domain must be unique within the environment. HP provides a set of pre-defined ranges that are reserved for use by Virtual Connect and will not conflict with server factory default WWNs.

When using the HP-defined WWN ranges, be sure that each range is used only once within the environment.

Displaying FC fabrics

To display a list of all FC SAN fabrics, use the `show fabric` command:

```
>show fabric
```

Serial number (logical) settings

Virtual Connect Manager can be configured to use logical serial numbers and logical UUIDs with a server profile regardless of the type of physical server. With these configuration values, software licensed with one or both of these values can be migrated to new hardware without re-licensing.

Configuring serial number ranges

VC-defined

```
> set serverid Type=VC-Defined PoolId=5
```

Factory-Default

```
> set serverid Type=Factory-Default
```

When using the HP-defined serial number ranges, be sure that each range is used only once within the environment.

Server Profile setup

A Virtual Connect server profile is a logical grouping of attributes related to server connectivity that can be assigned to a server blade. With the Virtual Connect v1.10 and higher, the server profile can include MAC address, PXE, and network connection settings for each server NIC port and WWN, SAN fabric connection, and SAN boot parameter settings for each Fibre Channel HBA port. After being defined, the server profile can be assigned to any server blade within the Virtual Connect domain. A Virtual Connect domain can have a maximum of 64 Virtual Connect server profiles.

Virtual Connect provides the ability to configure PXE settings when using either VC Assigned or factory default MAC addresses. In addition, Use BIOS is a new option for PXE, which maintains the current settings as configured by RBSU.

Virtual Connect also provides the ability to override the Virtual Connect assigned MACs and/or WWNs when creating a new profile.

When a server profile is assigned to a server blade, the Virtual Connect Manager securely connects to the server blade, configures the NIC ports with the appropriate MAC addresses and PXE settings, and configures the FC HBA ports with the appropriate WWNs and SAN boot settings. In addition, the Virtual Connect Manager automatically connects the server blade Ethernet and Fibre Channel ports to the specified networks and SAN fabrics. This server profile can then be re-assigned to another server blade as needed, while maintaining the server's network and SAN identity and connectivity.

The Virtual Connect Manager can be configured so that server blades use server factory default MACs/WWNs or Virtual-Connect-administered MACs/WWNs. These administered values override the default MAC addresses and WWNs when a server profile is assigned to a server, and appear to pre-boot environments and host operating system software as the hardware addresses. To use administered MAC addresses, select a range of HP pre-defined or user-specified MAC addresses.

Be sure to review the following list of guidelines before creating and deploying server profiles:

- The server blade firmware and option card firmware must be at a revision that supports Virtual Connect profile assignment. See the HP website (http://www.hp.com/go/bladesystemupdates).
- Before creating the first server profile, select whether to use moveable, administered MAC addresses and WWNs or whether to use the local server blade factory default MAC addresses and WWNs.
- After an enclosure is imported into a Virtual Connect domain, server blades remain isolated from the networks and SAN fabrics until a server profile is created and assigned.
- Server blades must be powered off to receive (or relinquish) a server profile assignment when using Virtual Connect-administered MAC addresses, WWNs, or changing Fibre Channel boot parameters.
- FC SAN Connections are only shown in server profile screens when there is an HP Virtual Connect Fibre Channel Module in the enclosure managed by Virtual Connect. FC SAN Connections are added in pairs and cannot be deleted. If an HP Virtual Connect Fibre Channel Module is added to a Virtual Connect domain that has existing profiles, an option to add FC connections appears in the existing profiles when editing.
- Some server profile SAN boot settings (controller boot order) are only applied by Virtual Connect after the server blade has been booted at least once with the final mezzanine card configuration.
- If PXE, controller boot order, or SAN boot settings are made outside of Virtual Connect (using RBSU or other configuration tools), Virtual Connect will restore the settings defined by the server profile after the server blade completes the next boot cycle.
- If using a QLogic HBA with some versions of Linux (RHEL3, RHEL4, SLES9, and SLES10), the HBA connection type must be set to "point to point only" in the adapter configuration settings in the QLogic BIOS utility or QLogic OS utility (if available). If the HBA settings are not changed, the HBA may be unable to log into the fabric and discover devices on the SAN.

Server profiles are associated with a specific enclosure device bay. After a profile is assigned, the Virtual Connect Manager configures the server blade in that device bay with the appropriate MAC/PXE/WWN/SAN boot settings and connects the appropriate networks and fabrics. Server blades that have been assigned a profile and remain in the same device bay do not require further Virtual Connect Manager configuration during server or enclosure power cycle. They will boot and gain access to the network and fabric when the server and interconnect modules are ready.

If a server blade is inserted into a device bay already assigned a server profile, Virtual Connect Manager automatically updates the configuration of that server blade before it is allowed to power up and connect to the network.

If a server blade is moved from a Virtual Connect managed enclosure to a non-Virtual Connect enclosure, local MAC addresses and WWNs are automatically returned to the original factory defaults. This feature prevents duplicate MAC addresses and WWNs from appearing in the data center because of a server blade redeployment.

NOTE: If you are using server factory default MAC addresses WWNs and default Fibre Channel boot parameters, you do not have to power off a server to make any profile changes. If you are using HP assigned or user assigned MAC addresses or WWNs, you must power a server off when moving a profile to the server or away from the server.

Server profile overview

A Virtual Connect server profile is a logical grouping of attributes related to server connectivity that can be assigned to a server blade. The server profile can include MAC address, PXE, and network connection settings for each server NIC port and WWN, SAN fabric connection, and SAN boot parameter settings

for each Fibre Channel HBA port. After being defined, the server profile can be assigned to any server blade within the Virtual Connect domain. A Virtual Connect domain can have a maximum of 64 Virtual Connect server profiles.

Virtual Connect provides the ability to configure PXE settings when using either VC-assigned or factory default MAC addresses. In addition, Use BIOS is an option for PXE, which maintains the current settings as configured by RBSU.

Virtual Connect also provides the ability to either override the VC-assigned MAC addresses or WWNs or both when creating a new profile. See "Define Server Profile Screen."

When a server profile is assigned to a server blade, the Virtual Connect Manager securely connects to the server blade, configures the NIC ports with the appropriate MAC addresses and PXE settings, and configures the FC HBA ports with the appropriate WWNs and SAN boot settings. In addition, the Virtual Connect Manager automatically connects the server blade Ethernet and Fibre Channel ports to the specified networks and SAN fabrics. This server profile can then be re-assigned to another server blade as needed, while maintaining the server's network and SAN identity and connectivity.

The Virtual Connect Manager can be configured so that server blades use server factory default MACs/WWNs or Virtual-Connect-administered MACs/WWNs. These administered values override the default MAC addresses and WWNs when a server profile is assigned to a server, and appear to pre-boot environments and host operating system software as the hardware addresses. To use administered MAC addresses, select a range of HP pre-defined or user-specified MAC addresses. See "MAC address settings."

IMPORTANT: Be sure to review the following list of guidelines before creating and deploying server profiles.

- The server blade firmware and option card firmware must be at a revision that supports Virtual Connect profile assignment. See the HP website (http://www.hp.com/go/bladesystemupdates).
- Before creating the first server profile, select whether to use moveable, administered MAC addresses and WWNs or whether to use the local server blade factory default MAC addresses and WWNs.
- After an enclosure is imported into a Virtual Connect domain, server blades remain isolated from the networks and SAN fabrics until a server profile is created and assigned.
- Server blades must be powered off to receive or relinquish a server profile assignment when using Virtual Connect-administered MAC addresses or WWNs, or when changing Fibre Channel boot parameters. When using Flex-10, there are special considerations for server power.

IMPORTANT: Before assigning a profile, unassigning a profile, or modifying a profile, be sure to review the "Server blade power on and power off guidelines."

- When assigning a VC-Assigned serial number (logical), the server must be powered off.
- FC SAN connections are shown in server profile screens only when there is an HP Virtual Connect Fibre Channel Module in the enclosure managed by Virtual Connect. FC SAN connections are added in pairs and cannot be deleted. If an HP Virtual Connect Fibre Channel Module is added to a Virtual Connect domain with existing profiles, an option to add FC connections appears in the existing profiles during editing.
- Some server profile SAN boot settings (controller boot order) are applied by Virtual Connect only after the server blade has been booted at least once with the final mezzanine card configuration.

- If PXE, controller boot order, or SAN boot settings are made outside of Virtual Connect (using RBSU or other configuration tools), Virtual Connect will restore the settings defined by the server profile after the server blade completes the next boot cycle.
- To boot properly from SAN when using Linux and VMware ESX 3.0.1 and ESX 3.0.2, change the QLogic QMH2462 4Gb FC HBA connection option to 'point-to-point only' in the QLogic BIOS configuration utility. The Emulex LPe 1105-HP 4Gb FC HBA does not require using the 'point-to-point' connection option to boot properly from SAN.

Server profiles are associated with a specific enclosure device bay. After a profile is assigned, the Virtual Connect Manager configures the server blade in that device bay with the appropriate MAC/PXE/WWN/SAN boot settings and connects the appropriate networks and fabrics. Server blades that have been assigned a profile and remain in the same device bay do not require further Virtual Connect Manager configuration during a server or enclosure power cycle. They will boot and gain access to the network and fabric when the server and interconnect modules are ready.

If a server blade is inserted into a device bay already assigned a server profile, Virtual Connect Manager automatically updates the configuration of that server blade before it is allowed to power up and connect to the network.

If a server blade is moved from a Virtual Connect managed enclosure to a non-Virtual Connect enclosure, local MAC addresses and WWNs are automatically returned to the original factory defaults. This feature prevents duplicate MAC addresses and WWNs from appearing in the data center because of a server blade redeployment.

IMPORTANT: Before assigning a profile, unassigning a profile, or modifying a profile, be sure to review the "Server blade power on and power off guidelines."

Creating server profiles

To create a new server profile, use the `add profile` command:

```
>add profile MyProfile
```

After an enclosure is imported into a Virtual Connect domain, server blades that have not been assigned a server profile are isolated from all networks to ensure that only properly configured server blades are attached to data center networks.

A server profile can be assigned and defined for each device bay so that the server blade can be powered on and connected to a deployment network. These profiles can then later be modified or replaced by another server profile.

A server profile can also be assigned to an empty bay to allow deployment at a later date.

Adding enet-network connections to a profile

To add a new Ethernet network connection to an existing server profile, use the `add enet-connection` command:

```
>add enet-connection MyProfile network=MyNetwork pxe=enabled
```

To add a multiple network Ethernet connection on a server port, use the following commands:

```
>add enet-connection MyProfile pxe=enabled
>add server-port-map MyProfile:1 MyNetwork VlanID=100
```

If the domain setting for `SharedServerVlanID` is set to `true`, then the `VlanID` property cannot be modified. Instead, the name of the shared uplink set with which the network is associated is required.

```
>add server-port-map MyProfile:1 MyNetwork Uplinkset=MyUplinkset
```

Adding FC fabric connections to a server profile

To add a new FC SAN connection to an existing server profile, use the `add fc-connection` command:

```
>add fc-connection MyProfile fabric=SAN_5
```

Configuring IGMP settings

To set Ethernet IGMP snooping properties, use the `set igmp` command:

```
> set igmp enabled=true timeout=30
```

IGMP allows VC-Enet modules to monitor (snoop) the IP multicast membership activities and to configure hardware Layer 2 switching behavior of multicast traffic to optimize network resource usage. Currently only IGMP v1 and v2 (RFC2236) are supported.

The IGMP Snooping idle timeout interval is set to 260 seconds by default. This value is basically the "Group Membership Interval" value as specified by IGMP v2 specification (RFC2236). For optimum network resource usage, set the interval to match the configuration on the customer network's multicast router settings.

Assigning a server profile to device bay 1

To assign a server profile to a specific device bay, use the `assign profile` command:

```
>assign profile MyProfile enc0:1
```

When a profile is created and assigned to a multi-blade server, the profile is applied to all of the blades in the multi-blade server. Therefore, the profile should contain enough Ethernet and Fibre Channel connection entries for all of the ports on all of the blades in the multi-server.

Configuring MAC cache failover settings

- To configure MAC Cache Failover Settings, use the `set mac-cache` command:

  ```
  >set mac-cache enabled=true refresh=10
  ```

- To display MAC Cache Failover Settings, use the `show mac-cache` command:

  ```
  >show mac-cache
  ```

When a VC-Enet uplink that was previously in standby mode becomes active, it can take several minutes for external Ethernet switches to recognize that the c-Class server blades can now be reached on this newly-active connection. Enabling Fast MAC Cache Failover causes Virtual Connect to transmit Ethernet packets on newly-active links, which enables the external Ethernet switches to identify the new connection (and update their MAC caches appropriately.) This transmission sequence repeats a few times at the MAC refresh interval (5 seconds recommended) and completes in about 1 minute.

IMPORTANT: Be sure to set switches to allow MAC addresses to move from one port to another without waiting for an expiration period or causing a lock out.

Logging out of the CLI

To log out of the CLI, use the exit command:

```
>exit
```

Common management operations

The following table provides the syntax for the most commonly used management operations.

For detailed information on a particular command, see "Managed elements (on page 13)."

Operation	Examples
Display general domain settings	`>show domain`
Display predefined address pools	`>show domain addresspool`

Display interconnect modules	• Summary display
	`>show interconnect`
	• Detailed display
	`>show interconnect *`
	• Single module display
	`>show interconnect enc0:2`

Display overall domain status	`>show status`
Display stacking link configuration and status	`>show stackinglink`
Display the system log	`>show systemlog`

Display a list of servers in the domain	• Summary display
	`>show server`
	• Detailed display
	`>show server *`
	• Single server display
	`>show server enc0:1`

Display server profiles	• Summary display
	`>show profile`
	• Detailed display
	`>show profile *`
	• Single profile display
	`>show profile MyProfile`

Delete the domain configuration	`>delete domain`
Force a failover to the standby VC Manager	`>reset vcm - failover`
Power off server blades	`>poweroff server enc0:2` `>poweroff server *`
Power on server blades	`>poweron server enc0:1` `>poweron server *`
Reset a server blade	`>reboot server enc0:4` `>reboot server *`
Unassign a server profile from a device bay	`>unassign profile MyProfile`
Modify Ethernet network connection properties	`>set enet-connection MyProfile 1 pxe=disabled`
Modify FC fabric connections	`>set fc-connection MyProfile 2 speed=auto`

Resetting the Virtual Connect Manager

To reset the Virtual Connect Manager, use the `reset vcm` command:

```
>reset vcm
>reset vcm [-failover]
```

Administrator privileges are required for this operation.

If VC Ethernet Modules are configured for redundancy using a primary and secondary Ethernet module, the user can use this feature to manually change which Virtual Connect Ethernet Module hosts the Virtual Connect Manager. The feature can also force the Virtual Connect manager to restart without switching to the alternate Virtual Connect Ethernet module. This feature can be useful when troubleshooting the Virtual Connect manager. The network and FC processing of the Virtual Connect subsystem is not disturbed during the restart or failover of the Virtual Connect Manager.

If the command line option `-failover` is included in the `reset vcm` command and a Virtual Connect Ethernet secondary module is available, the command line displays the following message:

```
SUCCESS: The Virtual Connect Manager is being reset. Please wait...
```

The user is logged out of the session after approximately 1 minute. An attempted login to the same Virtual Connect Ethernet Module is rejected with the following message:

```
Virtual Connect Manager not found at this IP address.
```

If the user attempts to log in to the secondary I/O bay, they might receive the following error message during the attempted login:

```
Unable to communicate with the Virtual Connect Manager. Please retry
again later.
```

The login should succeed after the Virtual Connect Manager has restarted on this secondary Virtual Connect Ethernet module. Allow up to 5 minutes, depending on the enclosure configuration.

If the command line option `-failover` is not included in the `reset vcm` command or a Virtual Connect Ethernet module is not available in the alternate I/O bay, the command line displays the following message:

```
SUCCESS: The Virtual Connect Manager is being reset. Please wait...
```

The user is logged out of the session after approximately 1 minute. If the user attempts to re-login, they might receive the following error message during the attempted login:

```
Unable to communicate with the Virtual Connect Manager. Please retry
again later.
```

The login should succeed after the Virtual Connect Manager has restarted. Allow up to 5 minutes, depending on the enclosure configuration.

Technical support

Before you contact HP

Be sure to have the following information available before you call HP:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Product identification number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

HP contact information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (http://www.hp.com/hps).
- In other locations, see the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

Acronyms and abbreviations

CRC

cyclic redundant checks

DHCP

Dynamic Host Configuration Protocol

DNS

domain name system

EFI

extensible firmware interface

FC

Fibre Channel

HBA

host bus adapter

IGMP

Internet Group Management Protocol

iSCSI

Internet Small Computer System Interface

LDAP

Lightweight Directory Access Protocol

LESB

Link Error Status Block

LUN

logical unit number

MAC

Media Access Control

PXE

Preboot Execution Environment

SAN

storage area network

SOAP

Simple Object Access Protocol

SSH

Secure Shell

SSL

Secure Sockets Layer

UDP

User Datagram Protocol

UUID

universally unique identifier

VCM

Virtual Connect Manager

WWN

World Wide Name

WWPN

worldwide port name

Index

P

R

S

T

U

V

W