HP Virtual Connect Manager Command Line Interface for c-Class BladeSystem Version 3.51/3.60 User Guide

Abstract

This document contains user information for the HP Virtual Connect Manager version 3.51/3.60 CLI. 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.

Part Number: 677486-003
June 2012
Edition: 3

© Copyright 2012 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Contents

Introduction

What's new

The command line interface user guide contains the following changes for VC 3.51:

- The output for the `show server-port` command has been updated.

Changes from VC 3.30 to 3.51

Command	Changes	Virtual Connect 3.30	Virtual Connect 3.51
`show server-port`	This command now shows the link status for FlexNIC ports. The profile column has been removed. The profile associated with the FlexNIC ports is now displayed as part of the physical port information.	The FlexNIC port output columns were Adapter Type, Network, MAC Address, Fabric, Port, WWN, and Profile.	The FlexNIC port output columns are Status, Network, MAC Address, Fabric, Port, and WWN.

Virtual Connect overview

HP 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. Virtual Connect includes the following components:

- VC-Enet modules
  - 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 Virtual Connect FlexFabric 10Gb/24-port Module for BladeSystem c-Class, which provides the capability to configure Ethernet and FC/FCoE or iSCSI connections
- VC-FC modules
  - 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 between the server and the data center infrastructure so networks can communicate with pools of HP BladeSystem servers, and so you can upgrade, replace, or move server blades within the enclosures without changes being visible to the external LAN and SAN environments. The external networks connect to a shared resource pool of servers rather than to individual

servers. Virtual Connect cleanly separates server enclosure administration from LAN and SAN administration.

VCM is embedded on the VC-Enet module. You can access VCM through a web-based GUI or CLI. The Onboard Administrator provides a web link to the Virtual Connect GUI.

The VC modules support the HP BladeSystem c7000 Enclosure, the HP BladeSystem c3000 Enclosure, and all the server blades and networks contained within the enclosure. FlexFabric modules are only supported in BladeSystem c7000 enclosures and G6 or newer server blades with Virtual Connect firmware v3.15 and later.

VC-Enet modules enable connectivity to all brands of data center Ethernet switches. VC-Enet modules can also be directly connected to other types of devices, such as printers, laptops, rack servers, and network storage devices.

The VC-FC and FlexFabric modules enable connectivity of the enclosure to Brocade, Cisco, McDATA, or QLogic data center FC switches. Every FC fabric is limited in the number of switches it can support, but the VC-FC modules do not appear as switches to the FC fabric and do not count against FC fabric limits.

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 8 servers (or up to 16 servers if the double-dense option is enabled). For more information on the double-dense option, see "Double-dense server bay option" in the user guide. Within the domain, any server blade with the requisite LAN or SAN devices can access any LAN or SAN connected to a VC module, and a server blade of a given processor type (Integrity or X86) can be used as a spare for any server blade of the same processor type within the same enclosure, as long as the server has the requisite number and type of connections. Using network access groups feature, the network administrator can clearly define a separation of networks based on their allowed functionality and prevent the server administrator from assigning specific network combinations in the same server profile.

By stacking (cabling) the VC-Enet modules together within the domain and connecting the VC-FC or FlexFabric module FC uplinks on the same bay of all enclosures to the same FC switch, every server blade in the domain can be configured to access any external network or fabric connection. With this configuration, you can use VCM 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 while using the Domain Setup Wizard. There are 16 half-height or 8 full-height server bays in a c7000 enclosure. A combination of full-height and half-height servers can be used in the same enclosure.

Multiple enclosure domains are not supported on c3000 enclosures. The VC-Enet or FlexFabric 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. Since FC does not support stacking, the VC-FC or FlexFabric module FC uplinks on the same bay of all enclosures must be connected to the same FC switch to enable profile mobility.

The management interfaces for all enclosure Onboard Administrators and VC modules within the same VC domain must be on the same lightly loaded subnet and highly reliable network. Overloads or loss of connectivity can disable configuration attempts until the connectivity is re-established and synchronized with the domain. The Onboard Administrator IP addresses used must be configured to be static. The Onboard Administrator user credential for all enclosures must be consistent to enable VCSU firmware updates for VC modules in the remote enclosures. All FC-capable modules in the same horizontally adjacent bay pair (bays 1-2, 3-4, and so on) must be of the same type and position in all enclosures.

Multi-enclosure double-dense domains require similar and compatible VC-FC modules in bays 5, 6, 7, and 8 in all enclosures if FC connectivity is required. If a multi-enclosure double-dense configuration contains incompatible VC-FC modules in bays 5, 6, 7, or 8 in the local or remote enclosures, some or all of the compatible VC-FC modules in the remote enclosures might be designated INCOMPATIBLE after import.

Command line overview

The VCM Command Line Interface can be used as an alternative method for administering the VCM. Using the CLI can be useful in the following scenarios:

- You can develop tools that utilize VCM 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.
- You can batch commands using script files. These script files can be run manually or scheduled to run automatically.

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	Target management entity
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 and 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 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) must 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`. Separate multiple properties with spaces.

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 without the optional parameter, 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 to suppress interactive prompts.

Distinguish options from other command line elements by using a preceding hyphen (–). 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

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

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 enable script automation and better security, SSH public/private key-pairs can be generated and uploaded to the public key to the VC firmware. For example:

```
>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. For example:

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

The CLI enables you to enter multiple CLI commands in a single command-line invocation. This capability is useful when batching several commands together and executing them in a particular sequence, within the context of the same 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

The CLI supports command scripts that contain blank lines and comments. Support for comments and blank lines enables you to maintain descriptive notes within the configuration script.

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

```
#-----------------------------------------------------------------------
# This is my sample Virtual Connect Domain Configuration Script
# Revision 1.0.1.2
# February 15, 2012
#-----------------------------------------------------------------------


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

# Add VC-Enet Networks
add network MyNetwork
add network Network2

# Add 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

The `unassign profile` command includes the ability to unassign 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 appears for that server or 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 with the dedicated management shell. The shell is provided after you log in with valid credentials, and only accepts known VCM CLI commands as input. You can quit the shell by using the `exit` command. See the example of logging in to the interactive management shell 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 v3.51/3.60
(C) Copyright 2006-2012 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, you 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. See the example of how to use the non-interactive mode for CLI command execution below. In the example, the primary VCM is located at IP address 192.168.0.120.

```
->ssh Administrator@192.160.0.120 show enclosure
<command output displayed to user's screen>
```

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*.

Remote access to the Virtual Connect Manager

To access the VCM CLI remotely through any SSH session:

1. Using any SSH client application, start an SSH session to the Virtual Connect Manager.
2. When prompted, enter the assigned IP address or DNS name of the Virtual Connect Manager.
3. Enter a valid user name.
4. Enter a valid password. The CLI command prompt appears.
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.

To access the VCM CLI remotely through the Onboard Administrator CLI, run the `connect interconnect` command from the Onboard Administrator CLI.

Command output filtering

The CLI provides output filtering capabilities that enable you 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 following examples illustrate some common usage scenarios for output filtering:

Example 1: Displaying all enabled users

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

Example 2: Displaying all VC Ethernet modules

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

Example 3: Displaying all external uplinks 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
copy	Copy a configuration from one server profile to another server profile
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)
restore	Restore a file from a remote location
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
banner (on page 15)	Manage the login screen banner configuration
config (on page 16)	Display all commands for all objects defined in the domain
configbackup (on page 17)	Manage configuration backup and restore operations
devicebay (on page 19)	Display enclosure device bay information
domain (on page 19)	Manage general Virtual Connect domain settings and information
enclosure (on page 22)	Manage general enclosure settings and information
enet-connection (on page 23)	Manage Ethernet network connections
enet-vlan (on page 26)	Manage Ethernet VLAN connections
external-manager (on page 27)	Manage external manager settings and information
fabric (on page 29)	Manage Fibre Channel SAN fabrics

Managed element	Description
fc-connection (on page 31)	Manage Fibre Channel SAN fabric connections
fcoe-connection (on page 34)	Manage FCoE SAN fabric connections
firmware (on page 37)	Manage interconnect module firmware
igmp (on page 37)	Manage Ethernet IGMP Snooping settings
igmp-group (on page 38)	Display interconnect module IGMP Group table information
interconnect (on page 38)	Manage I/O interconnect modules
interconnect-mac-table (on page 40)	Display interconnect module MAC table information
iscsi-boot-param (on page 40)	Manage iSCSI boot parameters
iscsi-connection (on page 43)	Manage iSCSI connections
ldap (on page 46)	Manage LDAP configuration settings
ldap-certificate (on page 47)	Manage LDAP certificate information
ldap-group (on page 48)	Manage LDAP group configuration settings
link-dist-interval (on page 49)	Manage the FC login re-distribution interval
lldp (on page 50)	Display LLDP information received on a port
log-target (on page 50)	Manage remote log destination settings
loop-protect (on page 52)	Manage network loop protection settings
mac-cache (on page 53)	Manage Ethernet MAC cache failover settings
nag-network (on page 54)	Manage network access group memberships
network (on page 55)	Manage Virtual Connect Ethernet networks
network-access-group (on page 59)	Manage network access groups
network-range (on page 60)	Manage ranges of networks
port-monitor (on page 63)	Monitor port monitor configurations
profile (on page 65)	Manage Virtual Connect server profiles
radius (on page 69)	Manage RADIUS authentication settings
radius-group (on page 70)	Manage RADIUS group configuration settings
role (on page 72)	Manage user authentication order by access role (privilege)
server (on page 73)	Manage physical HP BladeSystem server blades
serverid (on page 75)	Manage virtual server ID configuration settings
server-port (on page 76)	Display all physical server ports
server-port-map (on page 76)	Manage shared server downlink port mapping configuration
server-port-map-range (on page 78)	Manage ranges of shared server downlink port mapping configurations
snmp (on page 79)	Modify SNMP configurations
snmp-trap (on page 80)	Modify SNMP-trap configurations
ssh (on page 83)	Manage SSH configuration and information
ssl (on page 84)	Manage SSL configuration and Information
ssl-certificate (on page 84)	Manage SSL certificate information
ssl-csr (on page 85)	Manage an SSL certificate signing request
stackinglink (on page 86)	Display stacking link information and status
statistics (on page 86)	Display or reset statistics on a designated interconnect module port
statistics-throughput (on page 88)	Manage the port throughput statistics
status (on page 88)	Display overall Virtual Connect domain status information
storage-management (on page 89)	Manage iSCSI storage management information

Managed element	Description
supportinfo (on page 90)	Manage Virtual Connect support information
systemlog (on page 91)	Display Virtual Connect Manager system event log
tacacs (on page 91)	Manage TACACS+ authentication settings
uplinkport (on page 92)	Manage interconnect module uplink ports
uplinkset (on page 95)	Manage shared uplink port sets
user (on page 97)	Manage local Virtual Connect user configurations
user-security (on page 98)	Manage user security settings
vcm (on page 99)	Manage the Virtual Connect domain manager
version (on page 15)	Display CLI version information

The following sections provide detailed information on how to use the subcommands with each managed element.

To display command help, enter a command followed by `?` or `-help`. For more information on the `help` subcommand, see "Help subsystem (on page 104)."

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)

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

banner

Manage the login screen banner configuration.

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

Item	Description
`add banner`	Add banner text to the login screen. You can access VCM through ssh or the OA. After banner text is added, the banner is displayed before the user credential prompt when VCM is accessed.
Syntax	`add banner text=[”<banner text>”|’<banner text>’]`
Properties	
`text (required)`	The text to display on the login in screen. Multi-line banner text can be entered through multiple `add banner` commands. New lines are appended to existing text. The banner text limit is 1500 bytes. If the accumulated banner text length exceeds 1500 bytes, either from one or multiple `add banner` commands, an error message appears. Only printable characters are allowed.
Examples	
	`->add banner text="This is a private system, unauthorized access is not allowed."` Adds banner text with a single command

	`->add banner text="This is a private system."`
	`->add banner text=""`
	`->add banner text="Unauthorized access is prohibited."`
	`->add banner text=""`
	`->add banner text="Communications are monitored."`
	Adds banner text with multiple commands (A blank line is displayed in between each line of text in this example.)

Item	Description
`remove banner`	Remove configured banner text.
Syntax	`remove banner`
Example	
	`->remove banner` Removes the configured banner text

Item	Description
`show banner`	Display the configured banner text.
Syntax	`show banner`
Example	
	`->show banner` Displays the configured banner text

config

Display all CLI commands for all objects defined in the domain. The `show config` command is useful for generating a CLI script that can be used for creating a domain configuration. The generated script is only valid for the firmware version currently running. A script generated on one version of firmware is unlikely to be properly executed by a different version of firmware.

There are no bulk commands. Using the generated CLI script to create a large configuration with more than 300 networks is not recommended, as it can take a long time unless you rewrite the script to use the bulk commands.

Any user- or VC-defined MAC addresses, WWNs, and logical serial numbers will not appear in the output to avoid duplicating these values.

Supported actions: `help, show`

Item	**Description**
`show config`	Generate a configuration script from the running domain.
Syntax	`show config`
Example	
	`->show config` Displays the configuration script for the running domain

configbackup

Manage the domain configuration file.

Supported actions: `help, restore, save`

Item	**Description**
`restore configbackup`	Transfer a configuration file from a remote TFTP or FTP server and restore the configuration. Be sure that the domain state is IMPORTED before attempting to restore the configuration.
Syntax	`restore configbackup [-quiet][-maskEncryptKey] address=<tftp://ipaddress/[filename] | ftp://user:password@ipaddress/[filename]> [encryptionkey=<secret password>] [ignoreenclosureid=<true|false>] [ignorefwversion=<true|false>]`
Option	
`quiet (optional)`	Suppresses user confirmation prompts
`maskEncryprtKey (optional)`	Enables you to interactively specify the encryption key as a masked string at the command prompt
Properties	
`Address (required)`	A valid IP address of a TFTP or FTP server with user name and password (where needed) and the name of the configuration backup file. If not specified, the default file name is "vc-config-backup". The file path specified is treated as relative to the login directory for the user on the FTP server. Be sure that the permissions are appropriate for a successful transfer.
`EncryptionKey (optional)`	A password used to encrypt the configuration backup file
`IgnoreEnclosureID (optional)`	Restores a configuration that was generated on another enclosure. Valid values are "true" and "false". The default value is "false". When the value is set to "false", the configuration generated on another enclosure is rejected.
`IgnoreFWVersion (optional)`	Restores a configuration that was generated on another firmware version. Valid values are "true" and "false". The default value is "false". When the value is set to "false", the configuration generated on another firmware version is rejected.
Example	
	`->restore configbackup address=tftp://192.168.10.12/<filename>` Restores a configuration backup file from a remote TFTP server
	`->restore configbackup address=ftp://user:password@192.168.10.12/<filename>` Restores a configuration backup file from a remote FTP server

Item	Description
	->restore configbackup address=ftp://user:password@192.168.10.12/<filename> ignoreenclosureid=true Restores a configuration backup file from a remote FTP server and ignores the serial number
	->restore configbackup address=ftp://user:password@192.168.10.12/<filename> ignorefwversion=true Restores a configuration backup file from a remote FTP server and ignores the firmware version
	->restore configbackup address=ftp://user:password@192.168.10.12/<filename> encryptionkey=secret Restores a configuration backup file from a remote FTP server with an encryption key
	->restore configbackup -maskEncryptKey address=ftp://user:password@192.168.10.12/<filename> Restores a configuration backup file from a remote FTP server with a masked encryption key
	->restore configbackup -quiet address=ftp://192.168.10.12/<filename> Restores a configuration backup file without user confirmation prompts

Item	Description
save configbackup	Generate and transfer a Virtual Connect configuration backup file to a remote TFTP or FTP server.
Syntax	save configbackup [-maskEncryptKey] address=<tftp://ipaddress/[filename] | ftp://user:password@ipaddress/[filename]> [encryptionkey=<secret password>]
Option	
maskEncryprtKey (optional)	Enables you to interactively specify the encryption key as a masked string at the command prompt
Properties	
Address (required)	A valid IP address of a TFTP or FTP server with user name and password (where needed) and the name of the configuration backup file. If not specified, the default file name is "vc-config-backup". The file path specified is treated as relative to the login directory for the user on the FTP server. Be sure that the permissions are appropriate for a successful transfer.
EncryptionKey (optional)	A password used to encrypt the configuration backup file
Examples	
	->save configbackup address=tftp://192.168.10.12/<filename> Saves a configuration backup file to a remote TFTP server
	->save configbackup address=ftp://user:password@192.168.10.12/<filename> Saves a configuration backup file to a remote FTP server
	->save configbackup address=ftp://user:password@192.168.10.12/<filename> encryptionkey=secret Saves a configuration backup file to a remote FTP server with an encryption key

Item	Description
	->save configbackup -maskEncryptKey address=ftp://user:password@192.168.10.12/<filename> Saves a configuration backup file to a remote FTP server with a masked encryption key

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. Use "*" to display detailed information for all enclosures. 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, 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 device bay 2 of the local enclosure
	->show devicebay enc1:4 Displays detailed information for device bay 4 of a remote enclosure
	->show devicebay enc0:5 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 is 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.

Item	Description
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, a valid IP address and subnet mask must be configured. If disabled, 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 (Required if DomainIP is enabled)`	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 and 9, for 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, for 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, for 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 from 1 to 64. This property is valid only 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 valid only 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 valid only 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 from 1 to 64. This property is valid only if the WwnType is set to "VC-Defined". If not specified, the default pool ID is 1.

Item	Description
`WwnStart (Required if WwnType is User-Defined)`	The starting WWN address in a custom user-defined range. This property is valid only 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 valid only 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
	`->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 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 [<IPv4Address|DNSname>] [UserName=<username>] [Password=<password>] [DoubleDense=<True|False>]` For enclosures that are not imported, the password field is optional. If not specified, the system interactively prompts you for the password.
Parameter	
`IpAddress (Optional)`	The IPv4 address or DNS name of the remote enclosure to be imported. If not specified, the local enclosure is assumed.
Option	
`quiet`	This option suppresses user confirmation prompt while importing a remote enclosure, and is typically used in automated scripting scenarios.
Properties	
`UserName (Required for enclosures that are not imported)`	A valid user name with access to the Onboard Administrator for the enclosure to import. The user must have full administrative rights to all enclosure elements, such as device bays, I/O bays, and OAs).
`Password (Required)`	A valid OA user password for importing the enclosure. If no password is specified, the system interactively prompts you for a password during the import operation.
`DoubleDense (Optional)`	This setting can only be specified during the import of the local enclosure, and it affects the behavior of all other enclosures imported later. If the enclosure being imported supports double-dense servers, this property enables the device bay display format to display double-dense servers. The default behavior is to display 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 2001::34/64 UserName=admin password=am123` Imports a remote enclosure into the domain
	`->import enclosure` Imports the previously discovered local enclosure
	`->import enclosure 192.168.0.120` Imports a previously discovered remote enclosure

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	

Item	Description
`EnclosureID (required)`	The enclosure ID of the remote enclosure to be removed from the domain. Use "*" to remove all remote enclosures 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	
`EnclosureID (optional)`	The ID of an enclosure in the domain. If specified, only details for that enclosure appear.
Examples	
	`->show enclosure` Displays a summary 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", 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 not specified, the default is "UseBios". Only one connection can have PXE enabled per profile.

Item	Description
`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, both an Ethernet MAC Address and iSCSI MAC Address must also be specified. Valid values include "Factory-Default" and "User-Defined". IMPORTANT: "User-Defined" addresses within the domain address pool range are permanently depleted from the pool and can only be re-used as "User-Defined". Deleting the profile does not return the address to the pool. Deleting the domain is the only way to return "User-Defined" addresses to the pool.
`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 "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", you can configure a 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 the Ethernet connection is removed
Example	
	`->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. This 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". This 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", you can configure a 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"
	`->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>. Use <ProfileName:*> to display all profile Ethernet connections. Use "*" to display all connections in the domain.
Examples	
	->show enet-connection * Displays all Ethernet connections in the domain
	->show enet-connection Profile1:* Displays all Ethernet connections of a profile named Profile1
	->show enet-connection Profile1:1 Displays a specific Ethernet connection of a profile named 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 [-quiet][SharedServerVLanId=<true|false>] [PrefSpeedType=<Auto|Custom>] [PrefSpeed=<speed>] [MaxSpeedType=<Unrestricted|Custom>] [MaxSpeed=<speed>] [VlanCapacity=<Legacy|Expanded>]
Option	
quiet	This option suppresses user confirmation prompt, and is typically used in automated scripting scenarios.
Properties	
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". 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 you to select any VC Ethernet network for the server Ethernet connections, and VLAN ID mappings can be modified to ensure uniqueness.
PrefSpeedType (optional)	The default connection speed for any Ethernet connection using multiple networks. Valid values include "Auto" and "Custom". "Custom" enables you 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)	The maximum connection speed for any Ethernet connection using multiple networks. Valid values include "UnRestricted" and "Custom". "Custom" enables you to configure the preferred speed. The default value is "Unrestricted".
MaxSpeed (required if MaxSpeedType is Custom)	The maximum connection speed for any Ethernet connection using multiple networks. Valid values range from 100Mb to 10Gb in 100Mb increments.

Item	Description
`VlanCapacity (optional)`	The VLAN capacity mode. Valid values include 'Legacy' and 'Expanded'. 'Legacy' mode allows up to 320 VLANs per module and 28 VLANs per server connection. All VC-Enet modules are supported. This is the default setting. 'Expanded' mode allows up to 1000 VLANs per domain and 162 VLANs per physical server port. 1/10Gb Ethernet modules are NOT supported.
`UplinkResources (optional)`	The number of VLAN translations allocated to the uplinks. This attribute can be set only when VlanCapacity is "Extended". Valid values range from 240 to 4080 in increments of 16 (enclosure) or 24 (rack). The default value is 640.
Examples	
	`->set enet-vlan SharedServerVLanId=true` Enables SharedServerVLanId
	`->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
	`->set enet-vlan VlanCapacity=Expanded` Sets the VLAN capacity mode to Expanded to allow for larger network configurations

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: `help, remove, 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, you must specify values for each MacType, WwnType, and ServerIdType. IMPORTANT: You must set the external manager enabled to "false" using the `set external-manager` command before using the `remove external-manager` command.
Syntax	`remove external-manager [-quiet] [UserName=<username>] [MacType=<Factory-Default| User-Defined>] [MacStart=<MAC 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.

Item	Description
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 valid only 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 valid only 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	

	`->show external-manager`
	`->set external-manager UserName=A17005068 Enabled=false`
	(where A17005068 is the username reported by the previous command)
	`->remove external-manager username=A17005068 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`
	Displays the username, disables the external manager, and then removes the external manager and releases the profile control

	`->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

Item	Description
`set external-manager`	Enable or disable the control of an existing external manager over the Virtual Connect domain.
Syntax	`set external-manager [-quiet] UserName=<username> Enabled=<true|false>`

Item	Description
Option	
`quiet`	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 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 fabric being added to the domain.
Properties	
`Bay (required)`	The specific interconnect bay number with which the fabric is associated.
`Ports (required)`	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 number to be added to the fabric, for example "1, 2, 3, 4" (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.
`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".

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

Item	Description
`set fabric`	Modify properties of an existing fabric. This command 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>]`
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".

Item	Description
	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.
`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 fabric information.
Syntax	`show fabric [<FabricName>|*]`
Parameter	
`Name (optional)`	Name of an existing fabric. Use "*" to display a detailed output of all fabrics in the VC domain. If not specified, a summary output of all fabrics appears.
Examples	
	`->show fabric` Displays a summary of all FC SAN fabrics
	`->show fabric *` 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. For more information, see "General requirements for adding FC or FCoE connections (on page 144)."
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

Item	Description
	name is not specified, the connection is marked as “Unassigned” and 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, 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", "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 "User-Defined" 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 connection to a profile
	`->add fc-connection MyNewProfile Fabric=SomeFabric Speed=4Gb` Adds a new FC SAN connection and configures the port speed
	`->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 being 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>`

Item	Description
	[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 being modified
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", "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".
BootPort (Required if the Boot Priority is either Primary or Secondary 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 (Required if the Boot Priority is either Primary or Secondary 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 an 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	

Item	Description
`ConnectionID (optional)`	The ID of an existing FC SAN connection. The ID format is <ProfileName:Port>. Use <ProfileName:*> to display all FC SAN connections of a profile. Use "*" to display all FC SAN connections in the domain.
Examples	
	`->show fc-connection` Displays all FC SAN connections in the domain
	`->show fc-connection Profile1:*` Displays all FC SAN connections of a profile named Profile1
	`->show fc-connection Profile1:1` Displays a specific FC SAN connection of a profile named Profile1

fcoe-connection

Manage FCoE connections.

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

Item	Description
`add fcoe-connection`	Add a new FCoE connection to an existing server profile. For more information, see "General requirements for adding FC or FCoE connections (on page 144)."
Syntax	`add fcoe-connection <ProfileName> [Fabric=<FabricName>] [SpeedType=<1Gb|2Gb|4Gb|8Gb|Custom|Disabled>] [CustomSpeed=<100Mb-10Gb>] [WWNAddressType=<Factory-Default|User-Defined>] [PortWWN=<WWN address>] [NodeWWN=<WWN address>] [MACAddressType=<Factory-Default|User-Defined>] [EthernetMac=<MAC 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 created on an FCoE module to associate with the connection. If the fabric name is not specified, the connection is marked as “Unassigned” and associated with a specific bay.
`SpeedType (optional)`	The requested operation speed for the server port. Valid values include "1Gb", "2Gb", "4Gb", "8Gb", "Custom", and "Disabled". The default value is "4Gb". If the SpeedType is "Custom", you can configure any speed from 100Mb to 10Gb in 100Mb increments.
`CustomSpeed (required if SpeedType is Custom)`	The user-defined speed for the server port. Valid values include 100Mb to 10Gb configured in 100Mb increments.
`WWNAddressType (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 "User-Defined" is specified, both a Port WWN and Node WWN must also be specified. Valid values include "Factory-Default" and "User-Defined".
`PortWWN (required if WWNAddressType is User-Defined)`	The user-defined Port WWN address to use for the connection. The PortWWN must be an unused WWN address.
`NodeWWN (required if WWNAddressType is User-Defined)`	The user-defined Node WWN address to use for the connection. The NodeWWN must be an unused WWN address.
`MACAddressType (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

Item	Description
	"User-Defined" is specified, EthernetMAC must also be specified. Valid values include "Factory-Default" and "User-Defined".
`EthernetMAC (required if MACAddressType is User-Defined)`	The user-defined Ethernet MAC address to use for the connection
Examples	
	`->add fcoe-connection MyNewProfile Fabric=SAN_5` Adds a new FCoE connection to a profile
	`->add fcoe-connection MyNewProfile Fabric=SomeFabric SpeedType=4Gb` Adds a new FCoE connection and configures the port speed
	`->add fcoe-connection MyNewProfile` Adds a new FCoE connection and leaves it unassigned
	`->add fc-connection MyNewProfile Fabric=MyFabric SpeedType=Custom CustomSpeed=5000` Adds a new FCoE connection and sets a custom speed of 5Gb
	`->add fcoe-connection MyNewProfile WWNAddressType=Factory-Default` Adds a new FCoE connection and uses factory-default WWN addresses
	`->add fcoe-connection MyNewProfile WWNAddressType=User-Defined PortWWN=50:06:0B:00:00:C2:62:00 NodeWWN=50:06:0B:00:00:C2:62:01` Adds a new FCoE connection and provides user-defined WWN addresses
	`->add fcoe-connection MyNewProfile MACAddressType=Factory-Default` Adds a new FCoE connection and uses factory-default MAC addresses
	`->add fcoe-connection MyNewProfile MACAddressType=User-Defined EthernetMAC=00-17-A4-77-00-00` Adds a new FCoE connection and provides a user-defined MAC address

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

Item	Description
`set fcoe-connection`	Modify an existing FCoE connection.
Syntax	`set fcoe-connection <ConnectionID> [Fabric=<FabricName>] [SpeedType=<1Gb|2Gb|4Gb|8Gb|Custom|Disabled>] [CustomSpeed=<100Mb-10Gb>] [BootPriority=<priority>] [BootPort=<portName>] [BootLun=<LUN>]`
Parameters	
`ConnectionID (required)`	The ID of an existing FCoE connection. The ID format is <ProfileName:Port>.

Item	Description
Properties	
`Fabric (optional)`	The name of the fabric to associate with the connection. The fabric being specified should be associated with the same bay as the FCoE connection.
`SpeedType (optional)`	The requested operational speed for the server. Valid values include "1Gb","2Gb", "4Gb", "8Gb", "Custom", and "Disabled". If the SpeedType is "Custom", you can configure a speed from 100Mb to 10Gb in 100Mb increments.
`CustomSpeed (required if the SpeedType is Custom)`	The user-defined speed for the server port. Valid values include 100Mb to 10Gb configured in 100Mb increments.
`BootPriority (optional)`	Controls whether the FCoE HBA port is enabled for SAN boot and affects the BIOS boot order. Valid values include "BIOS", "Primary", "Secondary", and "Disabled".
`BootPort` (Required if the Boot Priority is either Primary or Secondary)	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` (Required if the Boot Priority is either Primary or Secondary)	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 fcoe-connection MyProfile:1 Fabric=SAN_5` Changes the fabric of an FCoE SAN fabric connection
	`->set fcoe-connection RedProfile:2 Fabric=""` Sets a FCoE SAN fabric connection to "Unassigned"
	`->set fcoe-connection MyProfile:1 SpeedType=Custom CustomSpeed=5000` Modifies the FCoE connection and sets a custom speed of 5Gb
	`->set fcoe-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 fcoe-connection`	Display the FCoE connections associated with the server profiles.
Syntax	`show fcoe-connection [<ConnectionID>]`
Parameter	
`ConnectionID (optional)`	The ID of an existing FCoE connection. The ID format is <ProfileName:Port>. Use <ProfileName:*> to display all FCoE connections of a profile. Use "*" to display all FCoE connections in the domain.
Examples	
	`->show fcoe-connection` Displays all FCoE connections in the domain
	`->show fcoe-connection Profile1:*`

Item	Description
	Displays all FCoE connections of a profile named Profile1
	`->show fcoe-connection Profile1:1` Displays a specific FCoE connection of a profile named Profile1

firmware

Display the Virtual Connect interconnect module 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

igmp-group

Display interconnect module IGMP Group table information.

Supported actions: `help, show`

Item	Description
`show igmp-group`	Display interconnect module IGMP Group table information for the specified module.
Syntax	`show igmp-group <ModuleID>`
Parameter	
`ModuleID (required)`	The ID of the module for which to display the IGMP Group table. The ID is in the format of `<EnclosureID>:<BayNumber>`.
Example	
	`->show igmp-group enc0:1` Displays the IGMP Group information for the module in bay 1 of enclosure enc0

interconnect

Manage I/O interconnect modules.

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

Item	Description
`add interconnect`	Add an interconnect module to an imported enclosure.
Syntax	`add interconnect <module ID> type=<moduleName>`
Parameter	
`module ID(required)`	The bay identifier within an existing network in the domain. For example, bay 3 in the local enclosure has a module ID of enc0:3.
`module (required)`	The name of the interconnect module. Use: • `type=vcenet` for an HP 1/10Gb VC-Enet Module • `type=vcenet2` for an HP 1/10Gb-F VC-Enet Module • `type=vcenet3` for an HP VC Flex-10 Enet Module • `type=vcenet5` for an HP FlexFabric 10Gb/24-port Module • `type=vcfc` for an HP 4Gb VC-FC Module • `type=vcfc2` for an HP VC 8Gb 24-Port FC Module • `type=vcfc3` for an HP VC 8Gb 20-Port FC Module
Example	
	`->add interconnect enc0:3 module=vcenet5` Adds an HP VC FlexFabric 10Gb/24-port Module to bay 3 of enclosure enc0

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.
Syntax	`remove interconnect <ModuleID|*>`
Parameter	
`ModuleID(required)`	The ID of the module to remove. The ID format is `<EnclosureID>:<BayNumber>`. Use <EnclosureID:*> to remove all interconnect modules that are physically present in the enclosure from the domain. Use <*:BayNumber> to remove all interconnect modules in the

Item	Description
	specified bay that are not physically present in any enclosures from the domain. Use "*" to remove all interconnect modules that are not physically present in any enclosure from the domain. To display a list of the IDs corresponding to modules in the domain, use the `show interconnect` command.
Examples	
	`->remove interconnect enc0:2` Removes the interconnect module in 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 physically present in a specific enclosure
	`->remove interconnect *:2` Removes all interconnect modules in a specific bay from the domain that are not physically present in any enclosure

Item	Description
`set interconnect`	Modify the interconnect module host name setting.
Syntax	`set interconnect [-quiet] [<EnclosureID>:<BayNumber>] [<Hostname=new_hostname>]`
Option	
`quiet`	Suppresses user confirmation prompts. This option is useful when scripting operations.
Properties	
`EnclosureID`	The ID of the enclosure
`BayNumber`	The Virtual Connect IO bay number
`Hostname`	A string of characters that cannot be longer than 63 characters and must begin with an uppercase or lowercase alphabetic character. If the hostname parameter is set to "DEFAULT", the host name is set to the default VC host name. Host names beginning with "VCE" are reserved.
Examples	
	`->set interconnect enc0:1 Hostname="DevelopmentNetworks"` Sets the host name of interconnect bay 1 in enclosure enc0 to DevelopmentNetworks
	`->set interconnect enc0:2 Hostname="DEFAULT"` Resets the host name of interconnect bay 2 in enclosure enc0 to the factory default

Item	Description
`show interconnect`	Display all interconnect modules in the domain.
Syntax	`show interconnect [<ModuleID>|*]`
Parameter	
`ModuleID (optional)`	The ID of the interconnect module. Use “*” to display a detailed view of all modules in the VC domain. If not specified, a summary output of all modules appears.
Examples	
	`->show interconnect`

Item	Description
	Displays a summary 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

interconnect-mac-table

Display interconnect module MAC table information.

Supported actions: `help, show`

Item	Description
`show interconnect-mac-table`	Display interconnect module MAC table information for the specified module.
Syntax	`show interconnect-mac-table <ModuleID>`
Parameter	
`ModuleID (required)`	The ID of the module for which to display the MAC table. The ID is in the format of `<EnclosureID>:<BayNumber>`.
Examples	
	`->show interconnect-mac-table enc0:1` Displays the module MAC table for the module in bay 1 of enclosure enc0
	`->show interconnect-mac-table enc0:1 Port=d5` Displays only MAC addresses associated with the specified port for the module in bay 1 of enclosure enc0
	`->show interconnect-mac-table enc0:1 "MAC Address=00:50:56:4C:6E:39"` Displays which port(s) the MAC address is learned on for the module in bay 1 of enclosure enc0

iscsi-boot-param

Manage iSCSI boot parameters within a domain.

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

Item	Description
`remove iscsi-boot-param`	Remove all iSCSI boot parameters configured on the specified iSCSI connection.
Syntax	`remove iscsi-boot-param <ConnectionID>`
Parameter	
`ConnectionID (required)`	The ID of an existing iSCSI connection. The ID format is <ProfileName:Port>. To retrieve the port number of the iSCSI connection, use the `show profile <ProfileName>` command.

Item	Description
Example	
	`->remove iscsi-boot-param MyProfile1:1` Removes boot parameters configured on connection 1 of MyProfile1

Item	Description
`set iscsi-boot-param`	Configure the basic iSCSI boot parameters on the specified iSCSI connection.
Syntax	`set iscsi-boot-param <ConnectionID> [-maskSecret] [-maskMutualSecret] [BootOrder=<Primary|Secondary|Disabled|USE-BIOS>] [LUN=<Logical Unit number>] [InitiatorName=<Initiator name>] [InitiatorIP=<IP address>] [Mask=<Netmask>] [Gateway=<Gateway>] [VlanID=<Vlan Id>] [TargetName=<Target Name>] [TargetIP=<Primary Target IP>] [TargetPort=<Primary Target Port>] [TargetIP2=<Alternate Target IP>] [TargetPort2=<Alternate Target Port >] [Authentication=<None|CHAP|CHAPM>] [Username=<username>] [Secret=<secret password>] [MutualUsername=<username>] [MutualSecret=<Mutual secret password>] [iSCSIBootParamDHCP=<Enabled|Disabled>] [NetworkParamDHCP=<Enabled|Disabled>] [DHCPVendorID=<VendorID>]`
Parameter	
`ConnectionID (required)`	The ID of an existing iSCSI connection. The ID format is <ProfileName:Port>. To retrieve the port number of the iSCSI connection, use the `show profile <ProfileName>` command.
Options	
`maskSecret (optional)`	Enables you to interactively specify the CHAP secret password as a masked string at the command prompt.
`maskMutualSecret (optional)`	Enables you to interactively specify the mutual CHAP secret password as a masked string at the prompt.
Properties	
`BootOrder (optional)`	Enables or disables iSCSI boot. Valid values for enabling iSCSI boot include "Primary", "Secondary", or "USE-BIOS". The default value is "Disabled".
`LUN (optional)`	The LUN of the target, which identifies the volume to be accessed. Valid values for standard LUNs are 0 to 255 decimal values. Valid values for extended LUNs are 13- to 16-character hexadecimal values. The default value is 0.
`InitiatorName (required if ISCSIBootParamDHCP is "Disabled")`	The name used for the iSCSI initiator on the booting system. The initiator name length can be a maximum of 223 characters. If the initiator name string contains non-alphanumeric characters, it must be enclosed in quotation marks.
`InitiatorIP (required if Network ParamDHCP is "Disabled")`	The IPv4 address used by the iSCSI initiator. This value is in dotted decimal format.
`Mask (required if NetworkParamDHCP is "Disabled")`	The IP network mask used by the iSCSI initiator. This value is in dotted decimal format.
`Gateway (optional)`	The default IP route used by the iSCSI initiator. This value is in dotted decimal format.
`VlanID (optional)`	The VLAN number that the iSCSI initiator uses for all sent and received packets. Valid values range from 1 to 4094.

Item	Description
TargetName (required if ISCSIBootParamDHCP is "Disabled")	The name of the target from which to boot. The target name length is a maximum of 223 characters. If the name string contains non-alphanumeric characters, it must be enclosed in quotation marks.
TargetIP (required if ISCSIBootParamDHCP is "Disabled")	The primary IPv4 address of the iSCSI target.
TargetPort (optional)	The TCP port associated with the primary target IP address. The default value is 3260.
TargetIP2 (optional)	The alternate target IPv4 address to use if the primary target IP is unavailable.
TargetPort2 (required if TargetIP2 is specified)	The TCP port associated with the alternate target IP address. The default value is 3260.
Authentication (optional)	The initiator and target must agree on an authentication method, or the iSCSI initiator cannot log in to the target. Supported values include "None", "CHAP", and "CHAPM". The default value is "None".
Username (required if authentication type is CHAP or CHAPM)	The user name for authentication. The user name length is a maximum of 223 characters. If the name contains non-alphanumeric characters, it must be enclosed in quotation marks.
Secret (required if authentication type is CHAP or CHAPM)	The secret password for CHAP and CHAPM authentication. It is specified as a string or a long hex value (starting with 0x). This value must be at least 96 bits (12 bytes, 24 hex digits) and at most 128 bits (16 bytes, 32 hex digits) long. The CHAP secret password can be entered as clear text in the command or as a masked string at the prompt.
MutualUsername (required if authentication type is CHAPM)	The mutual user name for CHAPM authentication. The user name length is a maximum of 223 characters. If the name contains non-alphanumeric characters, it must be enclosed in double quotation marks.
MutualSecret (required if authentication type is CHAPM)	The mutual secret password for CHAPM authentication. The password should be specified as a string or a long hex value (starting with 0x). This value must be at least 96 bits (12 bytes, 24 hex digits) and at most 128 bits (16 bytes, 32 hex digits) long. The mutual secret password can be entered as clear text in the command or as a masked string at the prompt.
ISCSIBootParamDHCP (optional)	Enables the iSCSI option ROM to retrieve the iSCSI boot parameters from DHCP or through static configuration. Valid values are "Enabled' and "Disabled". The default value is "Disabled", which enables static configuration.
NetworkParamDHCP (optional)	Enables the iSCSI option ROM to retrieve the TCP/IP parameters from DHCP or through static configuration. Valid values are "Enabled" and "Disabled'. The default value is "Disabled", which disables DHCP and enables static configuration.
DHCPVendorID (required if ISCSIBootParamDHCP is "Enabled")	The string used to match the value in the Vendor Class ID field in the DHCP offer packet when retrieving iSCSI boot parameters.
Examples	

Item	Description
	`->set iscsi-boot-param MyProfile1:1 BootOrder=Primary Lun=100 InitiatorName="iqn.2009-09.com.someorg.iSCSI-Initiator" InitiatorIp=192.128.3.1 Mask=255.255.0.0 TargetName="iqn.2009-09.com.someorg.iSCSI-Target" TargetIp=192.128.3.2 TargetPort=40000 Authentication=CHAP Username=SomeUserName Secret=SomePassword123` Configures basic boot attributes on an iSCSI connection of profile MyProfile1
	`->set iscsi-boot-param MyProfile1:1 BootOrder=Primary ISCSIBootParamDHCP=Enabled NetworkParamDHCP=Enabled DHCPVendorID=SomeVendorIDValue` Configures iSCSI Boot attributes to be retrieved from DHCP
	`->set iscsi-boot-param MyProfile1:1 -maskSecret -maskMutualSecret Authentication=CHAPM Username=SomeUserName MutualUsername=SomeMutualUsername ISCSIBootParamDHCP=Enabled NetworkParamDHCP=Enabled DHCPVendorID=SomeVendorIDValue` Configures CHAP secret and CHAPM secret values as a masked string

Item	Description
`show iscsi-boot-param`	Display the basic iSCSI boot parameters configured on the specified iSCSI connection.
Syntax	`show iscsi-boot-param [<ConnectionID>]`
Parameter	
`ConnectionID (optional)`	The ID of an existing iSCSI connection. The ID format is <ProfileName:Port>. Use `show profile <ProfileName>` or `show iscsi-connection <profileName:*>` to display the port number of the iSCSI connection.
Examples	
	`->show iscsi-boot-param MyProfile1:1` Displays boot parameters configured on connection 1 of MyProfile1
	`->show iscsi-boot-param MyProfile1:*` Displays boot parameters configured on all connections of MyProfile1
	`->show iscsi-boot-param *` Displays boot parameters configured on all profiles in the domain

iscsi-connection

Manage iSCSI connections.

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

Item	Description
`add iscsi-connection`	Add a new iSCSI connection to an existing server VC profile. This command can be executed only if the current VC domain is managing one or more Flex-10 modules.
Syntax	`add iscsi-connection <ProfileName> [Network=<NetworkName>] [AddressType=<Factory-Default|User-Defined>] [iScsiMAC=<MAC Address>] [SpeedType=<Auto|Preferred|Custom>] [Speed=<speed>]`
Parameter	

Item	Description
`ProfileName (required)`	The name of an existing profile to which the new connection is being added
Properties	
`Network (optional)`	The name of an existing network to associate with the connection. If the network name is not specified or is unassigned, it can be assigned later.
`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, the iSCSI MAC address must be specified. Valid values include "Factory-Default" and "User-Defined".
`iScsiMAC (required if AddressType is User-Defined)`	The user-defined iSCSI MAC address to use for the connection.
`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 allocated but is constrained 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, the speed type defaults to "Auto". If the speed type is "Custom", you can configure a speed (using the `Speed` property) from 100Mb to the 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 from 100Mb to the MAX configured speed for the network in 100Mb increments.
Examples	
	`->add iscsi-connection MyNewProfile Network=SomeNetwork` Adds a new iSCSI connection to the profile
	`->add iscsi-connection MyNewProfile` Adds a new iSCSI connection and leaves it unassigned
	`->add iscsi-connection MyNewProfile AddressType=Factory-Default` Adds a new iSCSI network connection and uses factory-default addresses
	`->add iscsi-connection MyNewProfile AddressType=User-Defined iScsiMAC=00-17-A4-77-00-00` Adds a new iSCSI network connection and provides a user-defined MAC address
	`->add iscsi-connection MyProfile Network=MyNetwork SpeedType=Preferred` Adds a new iSCSI network connection and sets the speed to Preferred
	`->add iscsi-connection MyProfile Network=MyNetwork SpeedType=Custom Speed=2000` Adds a new iSCSI network connection and sets the speed to 2Gb

Item	Description
`remove iscsi-connection`	Remove the last iSCSI connection from the server VC profile. If no connections exist, an error message appears.
Syntax	`remove iscsi-connection <ProfileName>`
Parameter	
`ProfileName (required)`	The name of an existing profile from which the connection is being removed

Item	Description
Example	
	`->remove iscsi-connection MyProfile` Removes the last added iSCSI connection from the profile

Item	Description
`set iscsi-connection`	Modify the properties of a specified iSCSI connection.
Syntax	`set iscsi-connection <ConnectionID> [Network=<Network Name>] [SpeedType=<Auto|Preferred|Custom>] [Speed=<speed>]`
Parameters	
`ConnectionID (required)`	The ID of an existing iSCSI connection. The ID format is <ProfileName:Port>.
Properties	
`Network (optional)`	The name of an existing network to associate with the connection. If the network name is not specified or is unassigned, it can be assigned later.
`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 allocated, constrained 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", you can configure a speed (using the `Speed` property) from 100Mb to the 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 from 100Mb to the MAX configured speed for the network in 100Mb increments.
Examples	
	`->set iscsi-connection MyNewProfile:1 Network=SomeNetwork` Changes the network to a different one
	`->set iscsi-connection MyNewProfile:1 Network=""` Unassigns the network from the connection
	`->set iscsi-connection MyProfile:1 Network=MyNetwork SpeedType=Preferred` Modifies the speed to Preferred
	`->set iscsi-connection MyProfile:1 SpeedType=Custom Speed=2000` Modifies the iSCSI connection and sets the speed to 2Gb

Item	Description
`show iscsi-connection`	Display the iSCSI connections associated with the server profiles.
Syntax	`show iscsi-connection [<ConnectionID>]`
Parameter	
`ConnectionID (optional)`	The ID of an existing iSCSI connection. The ID format is <ProfileName:Port>. Use <ProfileName:*> to display all iSCSI connections of a profile. Use "*" to display all iSCSI connections in the domain.

Item	Description
Examples	
	`->show iscsi-connection` Displays all iSCSI connections in the domain
	`->show iscsi-connection Profile1:*` Displays all iSCSI connections of a profile named Profile1
	`->show iscsi-connection Profile1:1` Displays a specific iSCSI connection of a profile named Profile1

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=<IPv4Address|DNSname>] [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 might 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 you are 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 authenticating using directory services
`SearchContext2 (optional)`	Second searchable path used to locate the user when authenticating using directory services
`SearchContext3 (optional)`	Third searchable path used to locate the user when authenticating using directory services
`ServerAddress (optional)`	The IPv4 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 them

Item	Description
	`->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	
	`->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@IPv4Address/filename>`
	-or-
	`load ldap-certificate Address=<ftp://user:password@ipaddress> Filename=<name>`

Properties	
`Address (required)`	A valid IPv4 address or host name of the FTP server, including user name, password, and name of the certificate file on the server
`Filename (required)`	The name of the LDAP certificate file on the server. The filename can also be given separately. The file path given will be treated as relative to the login directory for the user on the FTP server. The user should ensure that the permissions are appropriate for the transfer to succeed.
Examples	
	`->load ldap-certificate Address=ftp://user:password@192.168.10.12/new-ldap.crt` Downloads LDAP certification from the remote FTP server
	`->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. Use "*" to remove all configured LDAP certificates.

Item	Description
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. Use "*" to display detailed output of all the LDAP certificates in the VC domain. If an LDAP certificate is not specified, a summary output of all the LDAP certificates appears.
Examples	
	`->show ldap-certificate` Displays a summary of all LDAP certificates
	`->show ldap-certificate *` 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 being added
Properties	
`Description (optional)`	An informational description for the new group being added
`Privileges (optional)`	A set of one or more privileges for the group. Valid values include any combination of "domain", "server", "network", and "storage". Separate multiple values with commas.
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. Use "*" to remove all LDAP groups.
Examples	
	`->remove ldap-group MyGroup` Removes a specified 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". Separate multiple values with commas.
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. Use "*" to display detailed information for all LDAP groups. If no value is specified, a summary of all groups displays.
Examples	
	`->show ldap-group` Displays a summary 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

link-dist-interval

Manage the FC login re-distribution interval.

Supported actions: `help, set, show`

Item	Description
`set link-dist-interval`	Set the FC login re-distribution interval for uplinks that are part of a fabric configured for Automatic login re-distribution.
Syntax	`set link-dist-interval Interval=<1-1800>`
Property	
`Interval (required)`	FC login re-distribution interval for uplinks (in seconds). Valid values include positive integers in the range 1 to 1800. The default is 30 seconds.
Example	
	`->set link-dist-interval interval=10` Sets the FC login re-distribution interval to 10 seconds

Item	Description
`show link-dist-interval`	Display the FC login re-distribution interval for uplinks that are part of a fabric configured for Automatic login redistribution.
Syntax	`show link-dist-interval`
Example	
	`->show link-dist-interval` Displays the FC login re-distribution interval

lldp

Display LLDP information received on a specified port.

Supported actions: `help, show`

Item	Description
`show lldp`	Display LLDP information received on the specified port.
Syntax	`show lldp <PortID>`
Parameter	
`PortID (required)`	The port ID of the port for which to display LLDP information. PortID is composed of `<EnclosureID>:<BayNumber>:<PortLabel>`. A listing of the possible uplink PortIDs can be obtained by entering the `show uplinkport` command. Module downlink PortLabels range from d1 through d16, depending on the enclosure configuration.
Example	
	`->show lldp enc0:1:X1` Displays LLDP information received on port X1 of the module in bay1 of enclosure enc0

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=IPv4Address|DNS> [Severity=<Critical|Error|Warning|Info>] [Transport=<TCP|UDP>] [Port=<1-65535>] [Security=<None|STunnel>] [Format=<RFC3164|ISO8601>] [State=<Enabled|Disabled>]`
Properties	
`Destination (required)`	The IPv4 address or the DNS name of the remote log destination
`Severity (optional)`	The 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 is set to "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>`
Parameter	
`ID (required)`	The index of the remote log destination to delete
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=<IPv4Address|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 to modify
Properties	

Item	Description
`Destination (optional)`	The IPv4 address or the DNS name of the previously configured remote log destination
`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 is set to "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 1 to use a new IP address

Item	Description
`show log-target`	Display the remote log destination settings.
Syntax	`show log-target [<ID|*>]`
Parameter	
`ID (optional)`	The index of the remote log destination to view. Use "*" to display detailed information for all 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`
Example	
	`->test log-target` Sends a test message all log-targets

loop-protect

Manage loop protection settings.

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

Item	Description
`reset loop-protect`	Reset and restart loop detection for all server ports in a “loop-detected” error condition.
Syntax	`reset loop-protect`
Example	
	`->reset loop-protect` Resets and restarts loop detection for all server ports in a “loop-detected” error condition

Item	Description
`set loop-protect`	Configure the loop protection settings.
Syntax	`set loop-protect [-quiet] Enabled=<true|false>`
Option	
`quiet (optional)`	Suppresses user confirmation prompts
Properties	
`Enabled (required)`	Enables or disables network loop detection and protection. Valid values include "true" and "false".
Example	
	`->set loop-protect Enabled=true` Enables loop protection

Item	Description
`show loop-protect`	Display the loop protection configuration and all Ethernet ports currently disabled due to protection enforcement.
Syntax	`show loop-protect`
Example	
	`->show loop-protect` Displays the current loop protection configuration and all Ethernet ports currently disabled due to protection enforcement

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 to 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`

Item	Description
	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

nag-network

Manage networks associated to network access groups.

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

Item	Description
`add nag-network`	Add one or more networks to a network access group. Any network access groups previously configured for the network remain.
Syntax	`add nag-network Nag=<nagName> Network=<NetName1>[,<NetName2>,...]|<NagNetworkID>`
Parameter	
`Nag (required if NagNetworkID is not specified)`	The name of an existing network access group
`Network (required if NagNetwork ID is not specified)`	The name of the networks to be added as members to the network access group, separated by commas. Do not use spaces unless they are enclosed in quotation marks.
`NagNetworkID`	The Nag name and Network of interest. The format is <NagName:NetworkName>. If this is specified then the Nag= and Network= parameters are not provided.
Examples	
	`->add nag-network Nag=DatabaseNetGroup Network=Net1,Net2,Net3` Adds networks Net1, Net2, and Net3 to the DatabaseNetGroup network access group
	`->add nag-network nag1:network1` Adds network network1 to the nag1 network access group

Item	Description
`remove nag-network`	Removes a network from a network access group.
Syntax	`remove nag-network <NagNetworkID> | Nag=<nagName> Network=<NetName1>[,<NetName2>,…]`
Parameter	
`NagNetworkID (required if Nag= Network= is not specified)`	The ID of an existing network to network access group association. The ID format is <NagName:NetworkName>. The NagName must be specified if it is the only network access group of which the network is a member.
`Nag (required if NagNetworkID is not specified)`	The name of an existing network access group
`Network (required if NagNetworkID is not specified)`	The name of the network members to be removed from the network access group, separated by commas. Do not use spaces unless enclosed in quotation marks.

Item	Description
Examples	

	`->remove nag-network DatabaseNetGroup:Net1`
	-or-
	`->remove nag-network Nag=DatabaseNetGroup Network=Net1`
	Removes a specified network from a specified network access group

	`->remove nag-network Nag=DatabaseNetGroup Network=Net1,Net2` Removes specified networks from a specified network access group

Item	Description
`show nag-network`	Display the network to network access group association information.
Syntax	`show nag-network [<NagNetworkID>|*]`
Parameter	
`NagNetworkID (optional)`	The ID of an existing network to network access group association. The ID format is <NagName:NetworkName>. Use "*" to display detailed information for all network to network access group associations in the domain. If not specified, a summary of all network to network access group associations appears.
Examples	
	`->show nag-network` Displays a summary of all network to network access group associations in the domain
	`->show nag-network *` Displays detailed information for all network to network access group associations in the domain
	`->show nag-network DatabaseNetGroup:Net1` Displays detailed information about the association between a specified network access group and a specified network

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 is created, uplink ports can be added if the network is not using a shared uplink set. The SmartLink property is no longer supported during the creation of the network. If specified, it is ignored. To configure the SmartLink attribute, use the `set network` command.
Syntax	`add network <NetworkName> [-quiet] [Nags=<nagName>[,<nagName2>,...]] [UplinkSet=<UplinkSetName> VLanID=<VLanID>] [State=<Enabled|Disabled>] [NativeVLAN=<Enabled|Disabled>] [Private=<Enabled|Disabled>] [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. Valid characters include alphanumeric, "_", and ".". The maximum length of the name is 64 characters.
Option	
`Quiet`	Suppresses user confirmation prompts during network creation and modification. This

Item	Description
	option is used mainly in automated scripting scenarios.
Properties	
`Nags (optional)`	The names of the existing network access groups of which this network is a member, separated by commas. Do not use spaces unless they are enclosed in quotation marks. If no network access groups are specified, the domain default network access group (Default) is used.
`UplinkSet (optional)`	The name of an existing shared uplink set to use with this network. If this property is specified, 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 the shared uplink 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)`	The default connection speed for any Ethernet connection attached to this network. Valid values include "Auto" and "Custom". "Custom" enables you 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 you to configure the preferred speed. The default value is "Unrestricted".
`MaxSpeed (required if MaxSpeedType 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 as a member of the Default network access group
	`->add network Network1 nags=DatabaseNetGroup,AccessNetGroup` Creates a network named Network1 and assigns it to network access groups DatabaseNetGroup and AccessNetGroup
	`->add network MyNewNetwork2 UplinkSet=MyUplinkSet VLanID=145` Creates a new network and uses a shared uplink port set
	`->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

Item	Description
	`->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 a maximum connection speed of 6Gb

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

Item	Description
`set network`	Modify an existing Ethernet network.
Syntax	`set network <NetworkName> [-quiet] [State=<Enabled|Disabled>] [SmartLink=<Enabled|Disabled>][NativeVLAN=<Enabled|Disabled>] [Private=<Enabled|Disabled>] [Nags=<nagName>[,<nagName2>,...]] [Name=<NewName>] [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".
`SmartLink (optional)`	Enables or disables the SmartLink capability for a network. 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".
`Nags (optional)`	Modifies the network access groups of which this network is a member. The specified network access groups replace the original network access groups. If no network

Item	Description
	access groups are specified, the network access groups are not changed.
`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. Valid values are "Enabled" and "Disabled". 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)`	The default connection speed for any Ethernet connection attached to this network. Valid values include "Auto" and "Custom". "Custom" enables you 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 you to configure the preferred speed. The default value is "Unrestricted".
`MaxSpeed (required if MaxSpeedType 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 the specified 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 Nags=NetworkGroup2,NetworkGroup3` Changes the network access groups for Network1 to network access groups NetworkGroup2 and NetworkGroup3 (previous network access groups are removed)
	`->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
	`->set network Network1 PrefSpeedType=Custom PrefSpeed=4000 MaxSpeedType=Custom MaxSpeed=6000` Modifies the network to a preferred connection speed of 4Gb and a maximum connection speed of 6Gb

Item	Description
`show network`	Display all Ethernet networks in the domain. Configured values for ConnectionMode and VLanTunnel display for UNSHARED networks only. Configured values for NativeVLAN, UplinkSet, and VLanID display for SHARED

Item	Description
	networks only.
Syntax	`show network [<NetworkName>|*]`
Parameter	
`NetworkName (optional)`	The name of an existing network in the VC domain. Use "*" to display a detailed view of all the networks. If not specified, a summary view of the networks appears.
Examples	
	`->show network` Displays a summary of all networks
	`->show network *` Displays detailed information for all networks
	`->show network MyNetwork` Displays detailed information for a specific network

network-access-group

Manage network access groups.

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

Item	Description
`add network-access-group`	Create a new network access group. After the network access group is created, it can be added to a network. The maximum supported number of network access groups is 128.
Syntax	`add network-access-group <Name>`
Parameter	
`Name (required)`	The unique name of the new network access group to create. Valid characters include alphanumeric, "_", "-", and ".". The maximum length of the name is 64 characters.
Example	
	`->add network-access-group DatabaseNetGroup` Creates a new network access group, and then adds it to the domain

Item	Description
`remove network-access-group`	Remove a network access group from the domain. To remove a network access group, it cannot be in use by any server profiles. A network access group cannot be deleted if it is the only one to which a network belongs. The Default network access group cannot be deleted.
Syntax	`remove network-access-group <Name|*>`
Parameter	
`Name (required)`	The name of an existing network access group in the domain. Use "*" to remove all removable network access groups.
Examples	
	`->remove network-access-group DatabaseNetGroup` Removes a specified network access group
	`->remove network-access-group *` Removes all removable network access groups

Item	Description
`set network-access-group`	Modify an existing network access group.

Item	Description
Syntax	`set network-access-group <Name> Name=<NewName>`
Parameter	
`Name (required)`	The name of an existing network access group to modify
Property	
`Name (required)`	The new name of the network access group
Example	
	`->set network-access-group NetGroup1 Name=NetGroup2` Changes the name of an existing network access group from NetGroup1 to NetGroup2

Item	Description
`show network-access-group`	Display all network access groups in the domain.
Syntax	`show network-access-group [<Name>|*]`
Parameter	
`Name (optional)`	The name of an existing network access group in the VC domain. Use "*" to display a detailed view of all the network access groups. If not specified, a summary view of all network access groups appears.
Examples	
	`->show network-access-group` Displays a summary of all network access groups
	`->show network-access-group *` Displays detailed information for all network access groups
	`->show network-access-group DatabaseNetGroup` Displays detailed information for a specific network access group

network-range

Manage multiple networks in a shared uplink set.

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

Item	Description
`add network-range`	Create multiple networks in a shared uplink set.
Syntax	`add network-range [-quiet] UplinkSet=<UplinkSetName> [NamePrefix=<prefix>] [NameSuffix=<suffix>] VLANIds=<VLAN range list> [State=<enabled|disabled>] [PrefSpeedType=<auto|custom>] [PrefSpeed=<100Mb-10Gb in 100Mb steps>] [MaxSpeedType=<unrestricted|custom>] [MaxSpeed=<100Mb-10Gb in 100Mb steps>] [Nags=<Name1>[<Name2>,...] [SmartLink=<enabled|disabled>] [Labels=<Label1>[<Label2>,...] [Color=<red|green|blue|orange|purple>]`
Options	
`quiet`	This option suppresses user confirmation prompts. This option is useful when scripting operations.
Properties	
`UplinkSet (required)`	The name of an existing shared uplink port set to use with the new networks

Item	Description
`VLANIds (required)`	A comma separated list of VLAN ranges. The VLAN IDs must not overlap or already be used in the uplink port set. The VLAN IDS are combined with the NamePrefix and NameSuffix properties (if any) to create the name for the networks.
`NamePrefix (optional)`	The string to prefix before the VLAN ID when naming the new networks. If omitted, no string is used to prefix the VLAN ID.
`NameSuffix (optional)`	The string to add after the VLAN ID when naming the new networks. If omitted, no string is added after the VLAN ID.
`State (optional)`	Enables or disables the networks. Valid values are "Enabled" and "Disabled". The default value is "Enabled".
`PrefSpeedType (optional)`	The default connection speed for any Ethernet connection attached to these networks. Valid values include "Auto" and "Custom". "Custom" enables you 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 these networks. Valid values range from 100Mb to 10Gb in 100Mb increments.
`MaxSpeedType (Optional)`	The maximum connection speed for any Ethernet connection attached to these networks. Valid values include "Unrestricted" and "Custom". "Custom" enables you to configure the preferred speed. The default value is "Unrestricted".
`MaxSpeed (required if MaxSpeedType is "Custom")`	The maximum connection speed for any Ethernet connection attached to these networks. Valid values range from 100Mb to 10Gb in 100Mb increments.
`Nags (optional)`	The network access groups to which the networks belong, separated by commas. Do not use spaces unless they are enclosed in quotation marks. If no network access groups are specified, the domain default network access group (Default) is used.
`SmartLink (optional)`	Enables or disables the SmartLink capability for the networks. Valid values include "Enabled" and "Disabled".
`Labels (optional)`	Labels assigned to these networks. Labels are used in the GUI to help with management of large numbers of networks. Labels can be assigned in the CLI, but are only used in the GUI. A maximum of 16 labels can be assigned.
`Color (optional)`	Color assigned to these networks. Color is used in the GUI to help with management of large numbers of networks. A color can be assigned in the CLI, but is only used in the GUI. Allowed colors are red, green, blue, purple, or orange.
Examples	
	`->add network-range UplinkSet=Alpha NamePrefix=Network NameSuffix=_A VLANIDs=1-100` Creates 100 networks in an existing uplink set
	`->add network-range UplinkSet=Alpha NamePrefix=Network NameSuffix=_A VLANIDs=101-110,115-119,130,4094,700-703` Creates non-contiguous networks in an existing uplink set

Item	Description
`remove network-range`	Remove multiple networks from a shared uplink set.
Syntax	`remove network-range [-quiet] UplinkSet=<UplinkSetName> VLANIds=<VLAN range list>`

Item	Description
Options	
quiet	Suppresses user confirmation prompts during network range removal. This option is used mainly in automated scripting scenarios.
Properties	
UplinkSet (required)	The name of the shared uplink set from which the networks are being removed
VLANIds (required)	The list of VLAN IDs (comma separated list of VLAN ID ranges) to be deleted from the shared uplink set. For this command, the shared uplink set and list of VLAN IDs identify the networks to be deleted, not the network names.
Example	
	->remove network-range UplinkSet=Alpha VLANIDs=1-10,15,21-30 Removes networks from an existing uplink set

Item	Description
set network-range	Change the configuration of multiple networks in a shared uplink set.
Syntax	set network-range [-quiet] UplinkSet=<UplinkSetName> VLANIds=<VLAN range list> [State=<enabled|disabled>] [PrefSpeedType=<auto|custom>] [PrefSpeed=<100Mb-10Gb in 100Mb steps>] [MaxSpeedType=<unrestricted|custom>] [MaxSpeed=<100Mb-10Gb in 100Mb steps>] [Nags=<Name1>[<Name2>,...] [SmartLink=<enabled|disabled>] [Labels=<Label1>[<Label2>,...] [Color=<red|green|blue|orange|purple>]
Options	
quiet	This option suppresses user confirmation prompts. This option is useful when scripting operations.
Properties	
UplinkSet (required)	The name of an existing shared uplink port set to use with the networks.
VLANIds (required)	A comma separated list of VLAN ranges that identify the networks in the shared uplink port set being modified.
State (optional)	Enables or disables the networks. Valid values are "Enabled" and "Disabled". The default value is "Enabled".
PrefSpeedType (optional)	The default connection speed for any Ethernet connection attached to these networks. Valid values include "Auto" and "Custom". "Custom" enables you 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 these networks. Valid values range from 100Mb to 10Gb in 100Mb increments.
MaxSpeedType (Optional)	The maximum connection speed for any Ethernet connection attached to these networks. Valid values include "Unrestricted" and "Custom". "Custom" enables you to configure the preferred speed. The default value is "Unrestricted".
MaxSpeed (required if MaxSpeedType is "Custom")	The maximum connection speed for any Ethernet connection attached to these networks. Valid values range from 100Mb to 10Gb in 100Mb increments.

Item	Description
`Nags (optional)`	The network access groups to which the networks belong, separated by commas. Do not use spaces unless they are enclosed in quotation marks. If nags is not specified, the network access groups are not changed.
`SmartLink (optional)`	Enables or disables the SmartLink capability for the networks. Valid values include "Enabled" and "Disabled".
`Labels (optional)`	Labels assigned to these networks. Labels are used in the GUI to help with management of large numbers of networks. Labels can be assigned in the CLI, but are only used in the GUI. A maximum of 16 labels can be assigned.
`Color (optional)`	Color assigned to these networks. Color is used in the GUI to help with management of large numbers of networks. A color can be assigned in the CLI, but is only used in the GUI. Allowed colors are red, green, blue, purple, or orange.
Example	
	`->set network-range UplinkSet=Alpha VLANIDs=1-10,21-30 SmartLink=Enabled` Changes the SmartLink setting for multiple networks

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 is 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 EnclosureID 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 the port speed. Speed restrictions apply.
`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.

Item	Description
`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 automatically disables port monitoring.
Syntax	`remove port-monitor AnalyzerPort=<PortID|*> MonitorPort=<PortID|*>`
Properties	
`AnalyzerPort`	The network analyzer port to be removed. Use "*" to remove all network analyzer ports from the configuration.
`MonitorPort`	The monitor port to be removed. Use "*" to remove all 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 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 the port 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 EnclosureID is not specified, the default enclosure is the local enclosure where the domain resides.

Item	Description
`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, copy, help, load, remove, save, set, show, unassign`

Item	Description
`add profile`	Create a new server profile. After the profile is created, the profile can be configured using the "set" subcommand, and additional network, fabric, and FCoE connections can also be added. The server profile can also be assigned to a device bay using the `assign` subcommand.
Syntax	`add profile <ProfileName> [-NoDefaultEnetConn] [-NoDefaultFcConn] [-NoDefaultFcoeConn] [Nag=<nagName>] [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	
`Nag (optional)`	The network access group for the profile. The default is the domain Default network access group.
`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`	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

Item	Description
User-Defined)	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 alphanumeric character. If no UUID is specified, 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 MyNewProfile2 Nag=DatabaseNetGroup Creates a new profile and associates it with the DatabaseNetGroup network access group
	->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
	->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 the monarch bay.
Option	
PowerOn	Powers on the server after the profile is assigned
Examples	
	->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
`copy profile`	Copy an existing profile configuration to another profile. The copied profile (destination profile) will be left unassigned.
Syntax	`copy profile <src_profile_name> <dest_profile_name>`
Parameter	
`src_profile_name (required)`	The name of the profile from which the configuration is being copied
`dest_profile_name (required)`	The name of the profile to which the configuration is being copied
Example	
	`->copy profile_server1 profile_server_new` Copies the configuration from profile_server1 to profile_server_new

Item	Description
`load profile`	Load a saved EFI data object from a remote ftp server on the network. The EFI data object is loaded into an existing server profile. The server profile must not be assigned to a server bay and it must not have an EFI data object present.

Syntax	`load profile <ProfileName> address=<ftp://user:password@ipaddress/filename>`
	-or-
	`load profile <ProfileName> address=<ftp://user:password@ipaddress> filename=<name>`

Parameter	
`ProfileName (required)`	An existing and unassigned profile with no EFI data
Properties	
`address (required)`	A valid IPv4 address or host name of the FTP server, including user name and password
`filename (required)`	The name of the file on the FTP server from where EFI data has to be loaded. The filename can also be mentioned separately. The file path given will be treated as relative to the login directory for the user on the FTP server. The user should ensure that the permissions are appropriate for the transfer to succeed.
Examples	
	`->load profile Profile_1 address=ftp://user:password@192.168.10.12/new-profile-data` Loads a saved profile EFI data object file from a remote server
	`->load profile Profile_1 address=ftp://user:password@192.168.10.12 filename=/new-profile-data` Loads a saved profile EFI data object file from a remote server

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. Use "*" to remove all existing profiles.
Examples	
	`->remove profile MyProfile` Removes a server profile by name

Item	Description
	`->remove profile *` Removes all server profiles

Item	Description
`save profile`	Save an EFI data object from an existing server profile. The server profile must not be assigned to a server bay.

Syntax	`save profile <ProfileName> address=<ftp://user:password@ipaddress/filename>`
	-or-
	`save profile <ProfileName> address=<ftp://user:password@ipaddress> filename=<name>`

Parameter	
`ProfileName (required)`	An existing and unassigned profile in the domain
Properties	
`address (required)`	A valid IP address, with username, password, and the name of the EFI data file that will be stored on the FTP server
`filename (required)`	The name of the EFI data file that will be stored on the FTP server. The filename can also be mentioned separately. The file path given will be treated as relative to the login directory for the user on the FTP server. The user should ensure that the permissions are appropriate for the transfer to succeed.
Examples	
	`->save profile Profile_1 address=ftp://user:password@192.168.10.12/new-profile-data` Transfer a profile EFI data object file to a remote server
	`->save profile Profile_1 address=ftp://user:password@192.168.10.12 filename=/new-profile-data` Transfer a profile EFI data object file to a remote server

Item	Description
`set profile`	Modify properties of an existing server profile.
Syntax	`set profile <ProfileName> [Name=<NewName>] [EFIState=absent] [Nag=<nagName>]`
Parameter	
`ProfileName (required)`	The current name of the profile to modify
Properties	
`Name (required)`	The new name of the server profile
`EFIState (required)`	Specifies the presence or absence of EFI state information
`Nag (optional)`	The new network access group for the server profile. If not specified, the profile's network access group is not changed.
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
	`->set profile Profile1 Nag=NetGroup1` Changes the profile's network access group to NetGroup1

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.
Syntax	`show profile [<ProfileName>|*]`
Parameter	
`ProfileName (optional)`	The name of an existing profile in the VC domain. Use "*" to display all existing profiles. If not specified, a summary of all profiles appears.
Examples	
	`->show profile` Displays a summary 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

radius

Manage RADIUS authentication settings.

Supported actions: `help, set, show`

Item	Description
`set radius`	Modify and test the Virtual Connect RADIUS authentication settings.
Syntax	`set radius [-test] [Enabled=<true|false>] [ServerAddress=<IP Address|DNS Name>] [Port=<portNum>] [ServerKey=<key>] [Timeout=<timeout>] [SecondaryServerAddress=<IP Address|DNS Name>] [SecondaryPort=<portNum>] [SecondaryServerKey=<key>] [SecondaryTimeout=<timeout>]`
Option	
`Test (optional)`	Tests the RADIUS configuration without applying changes
Properties	
`Enabled (optional)`	Enables or disables RADIUS authentication. Valid values include "true" and "false".
`ServerAddress (optional)`	The IP address or the DNS name of the primary RADIUS server used for authentication
`Port (optional)`	The server UDP port number. Valid values include a valid port number between 1 and 65535. The default port is 1812.
`ServerKey (optional)`	The plain-text string used to encrypt user details exchanged with the primary

Item	Description
	RADIUS server. It must match the server key configured for this VC on the primary server. RADIUS authentication will not work if the server key is blank or null.
`Timeout (optional)`	The time in seconds that VCM should wait before timing out the request. If the primary server times out and a secondary server is configured, VCM attempts the request on the secondary server. If the secondary server times out, the request fails. The valid range of values is from 1 to 600 seconds. The default timeout is 10 seconds.
`SecondaryServer Address (optional)`	The IP address or host name of the secondary RADIUS server used for authentication
`SecondaryPort (optional)`	The UDP port to use for RADIUS communication. Valid values include a valid port number between 1 and 65535. The default UDP port number is 1812.
`SecondaryServerKey (optional)`	The plain-text string used to encrypt user details exchanged with the secondary RADIUS server. It must match the server key configured for this VC on the secondary server. The RADIUS authentication will not work if the shared key is blank or null.
`SecondaryTimeout (optional)`	The timeout value in seconds for RADIUS communication with the secondary server
Examples	
	`->set radius -test Enabled=true ServerAddress=192.168.0.27` Tests the RADIUS configuration changes without applying them
	`->set radius Enabled=true ServerAddress=192.168.0.124 ServerKey=test123 SecondaryServerAddress=radserver.hp.com SecondaryServerKey=test456` Enables RADIUS authentication for users

Item	Description
`show radius`	Display the Virtual Connect RADIUS authentication settings.
Syntax	`show radius`
Example	
	`->show radius` Displays RADIUS information

radius-group

Manage Virtual Connect RADIUS groups.

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

Item	Description
`add radius-group`	Add a RADIUS group.
Syntax	`add radius-group <GroupName> [Description=<string>] [Privileges=<privileges>]`
Parameters	
`GroupName (required)`	The name of the RADIUS group being added. The name can consist of alphanumeric characters, hyphens (-), underscores (_) and periods (.). The maximum length of the name is 255 characters.
Properties	

Item	Description
`Description (optional)`	An informational description for the new group being added. The description can consist of 0 to 20 alphanumeric characters, dash (–), underscore (_), or period (.), backslash (\) and single-quote (').
`Privileges (optional)`	A set of one or more privileges for the group. Valid values include any combination of "domain", "server", "network", and "storage". Separate multiple values with commas. If privileges are not specified, then the group will have no privileges and can only view information. If '*' is specified, it indicates all privileges.
Example	
	`->add radius-group MyNewGroup Description="Test Group" Privileges=domain,server` Adds a new RADIUS group

Item	Description
`remove radius-group`	Remove an existing RADIUS group.
Syntax	`remove radius-group <GroupName|*>`
Parameter	
`GroupName (required)`	The name of an existing RADIUS group to be removed. Use "*" to remove all RADIUS groups.
Examples	
	`->remove radius-group MyGroup` Removes a specified RADIUS group
	`->remove radius-group *` Removes all RADIUS groups

Item	Description
`set radius-group`	Modify the properties of an existing RADIUS group.
Syntax	`set radius-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". Separate multiple values with commas.
Example	
	`->set radius-group MyGroup Description="Test Group" Privileges=domain,server,network` Modifies a RADIUS group description and privileges

Item	Description
`show radius-group`	Display the existing RADIUS groups.
Syntax	`show radius-group [<GroupName>|*]`
Parameter	
`GroupName (optional)`	The name of an existing RADIUS group in the domain. Use "*" to display

Item	Description
	detailed information for all RADIUS groups. If no value is specified, a summary of all groups appears.
Examples	
	`->show radius-group` Displays a summary of all RADIUS groups
	`->show radius-group MyGroup` Displays detailed information for a specific RADIUS group
	`->show radius-group *` Displays detailed information for all RADIUS groups

role

Manage role-based user authentication.

Supported actions: `help, set, show`

Item	Description
`set role`	Configure the authentication order for a VC role.
Syntax	`set role <RoleName> Order=<order>`
Parameter	
`RoleName (required)`	The VC privilege/role for which the existing authentication order is to be set. Valid values are "domain", "network", "server", and "storage".
Property	
`Order (required)`	The order of authentication to be set for a given role, specified as one or more authentication methods separated by a comma. The format is <method1,method2,method3>. Valid values are "ldap", "radius", "tacacs", and "local".
Examples	
	`->set role network Order=tacacs,radius` Sets the order for the network privilege to be TACACS+, followed by RADIUS
	`->set role server Order=ldap,radius,tacacs` Sets the order for the server privilege to be LDAP, followed by RADIUS, followed by TACACS+

Item	Description
`show role`	Display the current authentication order for a VC role.
Syntax	`show role [<RoleName>|*]`
Parameter	
`RoleName (optional)`	The name of a VC role for which the existing authentication order is to be displayed. Valid values are "domain", "server", "network", and "storage". Use "*" to display detailed information for all user roles. If not specified, a summary of all roles appears.
Examples	
	`->show role` Displays a summary authentication order of all user roles
	`->show role domain` Displays the authentication order for the domain user role

Item	Description
	->show role * Displays the authentication order for all user roles

server

Manage server blades.

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

Item	Description
poweroff server	Power off one or more physical servers.
Syntax	poweroff server <ServerID|*> [-Force|-ForceOnTimeout] [-timeout=<timeout>]
Parameter	
ServerID (required)	The ID of a physical server in the domain. The format of the server ID is <EnclosureID:DeviceBay>. If the EnclosureID is not specified, the local enclosure is used by default. Use "*" to power 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 operating system to shut down gracefully. Only use this option 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 (60 seconds by default), 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 Powers off the server in device bay 2 of the local enclosure
	->poweroff server enc0:2 -Force Forces the server in device bay 2 of the local enclosure to power off
	->poweroff server * Powers off all servers in the domain
	->poweroff server enc0:* Powers off all servers in the local 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 Powers off all servers and specifies a custom timeout of 3 minutes
	->poweroff server enc0:1 Powers off the multi-blade server in bays 1-4 of the local enclosure

Item	Description
poweron server	Power on one or more physical servers.
Syntax	poweron server <ServerID|*> [-Timeout=<timeout>]
Parameter	
ServerID (required)	The ID of a server in the domain. The format of the server ID is <EnclosureID:DeviceBay>. If the EnclosureID is not specified, the local

Item	Description
	enclosure is used by default. Use "*" to power 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	
`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 server in bay 2 of the local enclosure
	`->poweron server *` Powers on all servers in the domain
	`->poweron server enc0:*` Powers on all servers in the local enclosure
	`->poweron server * -Timeout=120` Powers on all servers in the domain and specifies a custom timeout of 2 minutes
	`->poweron server enc0:1` Powers on the multi-blade server in bays 1-4 of the local enclosure

Item	Description
`reboot server`	Reboot one or more physical servers.
Syntax	`reboot server <ServerID|*> [-Force] [-ForceOnTimeout] [-timeout=<timeout>`
Parameter	
`ServerID (required)`	The ID of a server in the domain. The format of the server ID is `<EnclosureID:DeviceBay>`. If the EnclosureID is not specified, the local enclosure is used by default. Use "*" to reboot 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 operating system to shut down gracefully. Only use this option 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 (60 seconds by default), 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 server in device bay 2 of the local enclosure
	`->reboot server enc0:2 -Force` Forces the server in device bay 2 of the local enclosure to reboot
	`->reboot server * -ForceOnTimeout -Timeout=180` Attempts a graceful shutdown, but forces a reboot on all servers after a timeout of 2 minutes
	`->reboot server *` Reboots all servers in the domain
	`->reboot server enc0:*` Reboots all servers in the local enclosure
	`->reboot server enc0:1` Reboots the multi-blade server in bays 1-4 of the local enclosure

Item	Description
`show server`	Display all servers in the domain.
Syntax	`show server <ServerID|*>`
Parameter	
`ServerID (optional)`	The ID of a server in the domain. The format of the server ID is `<EnclosureID:Bay>`. If the EnclosureID is not specified, the 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 of all servers
	`->show server *` Displays detailed information for all servers
	`->show server enc1:*` Displays detailed information for all servers in a remote enclosure
	`->show server enc0:4` Displays detailed information for the server in device bay 4 of the local enclosure
	`->show server enc0:5` Displays detailed information for the multi-blade server in bays 5-8 of the local enclosure

serverid

Manage virtual server ID configuration settings.

Supported actions: `help, set, show`

Item	Description
`set serverid`	Modify virtual server ID domain settings. The serial number attributes can be changed only in one of the following scenarios: • The virtual server ID source type is "Factory-Default". • The virtual server ID source type is "VC-Defined" or "User-Defined", but no profiles are using server IDs from this source. • The virtual server ID source type is "User-Defined", and the range is being extended by lowering the start value or increasing the end value.
Syntax	`set serverid Type=Factory-Default`
	`set serverid Type=VC-Defined [PoolID=<1-64>]`
	`set serverid Type=User-Defined Start=VCX01nnnnn End=VCX01nnnnn`
Properties	
`Type (required)`	The type of the virtual serial number source. When server profiles are created, the UUID values are not allocated from the pool, the virtual serial number is allocated from the pool; and the virtual UUID is randomly generated. 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

Item	Description
	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. If the port is unlinked and no connectivity exists, the cause is displayed. For more information about possible causes, see "Port status conditions (on page 148)."
Syntax	`show server-port [<PortID>]`
Parameter	
`PortID (Optional)`	The reference of a port mapping ID. The PortID format is `<EnclosureID:IOBay:Port>`. The PortID can be referenced from the ID column in the summary. The detailed display shows all FlexNICs that could be associated with a server port.
Examples	
	`->show server-port` Displays a summary 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
	`->show server-port enc0:1:d4` Displays detailed information for the Device Control Channel

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.
Syntax	`add server-port-map <ConnectionId> <Network Name> [Uplinkset=<Uplink Set Name>] [VLanID=<VLan ID>] [Untagged=<true|false>]`
Parameters	
`ConnectionID (required)`	The ID of an existing Ethernet 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 is 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 uplink set to use with the server port mapping. If the domain setting SharedServerVLanId is set to "true", Uplinkset is a required value.
`VLanID (optional)`	The VLAN ID to use for the mapping. Valid values include 1 to 4094. If the uplink set name is specified, 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 uplink set.
`Untagged (optional)`	Enables or disables the network to handle untagged packets. Only one network in an Ethernet network connection can handle untagged packets. The default value is "false". If a shared uplink set is used, 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 Uplinkset=MyUplinkset1 UnTagged=true` Adds a new server port to shared network mapping and enables untagged packet handling

Item	Description
`remove server-port-map`	Remove a server port network mapping.
Syntax	`remove server-port-map <ConnectionID|*> [<Network Name>]`
Parameters	
`ConnectionID (required)`	The ID of an existing Ethernet connection associated with a profile and a server port. The format of the ConnectionID is `<ProfileName:PortNumber>`. Use "*" to remove 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 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 network is associated with a shared uplink set.
Syntax	`set server-port-map <ConnectionID> <Network Name> [VLanID=<VLanID>] [UnTagged=<true|false>]`
Parameters	
`ConnectionID (required)`	The ID of an existing Ethernet 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 server port network mapping. 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 can handle untagged packets. The default value is "false". If a shared uplink set is 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", you must specify a VLanID if the global option SharedServerVLanId is set to "false".
Examples	
	`->set server-port-map MyProfile:1 Network1 VLanId=100` 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.
Syntax	`show server-port-map [<ConnectionID> | *]`
Parameter	
`ConnectionID (optional)`	The ID of an existing Ethernet connection associated with a profile and a server port. The format of the ConnectionID is `<ProfileName:PortNumber>`.
Examples	
	`->show server-port-map` Displays a summary of 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 server port mappings

server-port-map-range

Manage ranges of shared server downlink port mapping configurations.

Supported actions: `add, help, remove`

Item	Description
`add server-port-map-range`	Add a new server port network mapping range, and allow server ports to be shared among multiple VC Ethernet networks.
Syntax	`add server-port-map-range <ConnectionId> UplinkSet=<Uplink Set Name> VLANIDs=<VLAN ID Range List> [MatchUplinkSet=<true|false>]`

Item	Description
Parameters	
`ConnectionId (required)`	The ID of an existing Ethernet connection associated with a profile and a server port. The format of the ConnectionID is `<ProfileName:PortNumber>`.
Properties	
`Uplinkset (required)`	The name of the shared uplink set to use with the server port mapping
`VLANIDs (required)`	The VLAN IDs to use for the mapping. The format is a comma-separated list of VLAN ID ranges, where a range is either a single VLAN ID or a hyphen-separated pair of VLAN IDs that identify a range of VLAN IDs. Valid VLAN ID values include 1 to 4094.
MatchUplinkSet `(optional)`	Requires that the VLANs used for mappings match the VLAN IDs specified on the identified Uplink Set. If set to false, the command will not set the profile connection associated uplink set attribute (but will use the uplink set VLAN IDs from the uplink set). If there are already server port map entries for the specified profile connection, then either the uplink set must match or the port map entries must not have the associated uplink set attribute specified. The default value of this attribute is "false".
Examples	
	`->add server-port-map-range MyProfile:1 UplinkSet=MyUplinkSet1 VLanIds=101-124,214` Adds multiple networks to a server-port-map
	`->add server-port-map-range MyProfile:2 UplinkSet=MyUplinkSet2 VLanIds=1-20 MatchUplinkSet=true` Adds multiple networks to a server-port-map and locks VLANs to an uplink set

Item	Description
`remove server-port-map-range`	Remove one or more server port network mappings.
Syntax	`remove server-port-map-range <ConnectionId> VLANIds=<VLAN ID Range List>`
Parameters	
`ConnectionId (required)`	The ID of an existing Ethernet connection associated with a profile and a server port. The format of the Connection ID is `<ProfileName:PortNumber>`.
`VLANIDs (required)`	The list of VLAN IDs to be removed from the mapping. The format is a comma-separated list of VLAN ID ranges, where a range is either a single VLAN ID or a hyphen-separated pair of VLAN IDs that identify a range of VLAN IDs. Valid VLAN ID values include 1 to 4094.
Example	
	`->remove server-port-map-range MyProfile:1 VLanIds=151-170,215` Removes multiple server port network 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.

Item	Description
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".
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. You can configure up to five VC-Enet and five VC-FC SNMP trap destinations.

Item	Description
	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=<IPv4Address|DNSname> [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. If not specified, the default value is "public". For VC-Enet modules, the maximum string length is 39. For VC-FC modules, the maximum string length is 24.
`Format`	Format of the new trap. Valid values are "SNMPv1" and "SNMPv2". If not specified, the default is "SNMPv1".
`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 specified, 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, but the severities are applied to the domain categories.

Item	Description
`remove snmp-trap`	Removes a previously configured SNMP trap destination.
Syntax	`remove snmp-trap <Name|*>`
Parameter	

Item	Description
`Name (required)`	The name of the trap destination to be removed. Use "*" to remove all traps.
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=<IPv4Address|DNSname>] [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	
`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 specified, 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 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, 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, the SSH clients must be configured correctly to have access. This command loads an SSH key for the current user only. Other VC users are not able to use the same SSH key to authenticate. This command is only valid for local VC users (no LDAP, TACACS+, or RADIUS users).

Syntax	`load ssh Address=<ftp://user:password@IPv4Address/filename>`
	-or-
	`load ssh Address=<ftp://user:password@ipaddress> Filename=<name>`

Properties	
`Address (required)`	The IPv4 address or host name of an FTP server, with user name, password, and remote file containing the SSH keys to transfer.
`Filename (required)`	The name of the remote file containing the SSH keys to transfer. The filename can also be mentioned separately. The file path given will be treated as relative to the login directory for the user on the FTP server. The user should ensure that the permissions are appropriate for the transfer to succeed.
Examples	
	`->load ssh Address=ftp://user:password@192.168.10.12/ssh_key.pub` Transfers the SSH key from the remote FTP server
	`->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`
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 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 "Strong".
Examples	
	`->set ssl strength=strong` Enables strong SSL encryption
	`->set ssl strength=all` Enables default SSL encryption settings

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 resets.

Syntax	`load ssl-certificate Address=<ftp://user:password@IPv4Address/filename>`
	-or-
	`load ssl-certificate Address=<ftp://user:password@ipaddress> Filename=<name>`

Properties	
`Address (required)`	A valid IPv4 address or host name of the FTP server, with user name, password, and name of the SSL certificate file to transfer.
`Filename (required)`	The name of the SSL certificate file to transfer. The filename can also be mentioned separately. The file path given will be treated as relative to the login directory for the user on the FTP server. The user should ensure that the permissions are appropriate for the transfer to succeed.
Examples	
	`->load ssl-certificate Address=ftp://user:password@192.168.10.12/ my-new-ssl.crt` Transfers a new custom SSL certificate from the remote FTP server
	`->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. Use "*" to display detailed SSL certificate information.
Syntax	`show ssl-certificate [*]`
Examples	
	`->show ssl-certificate` Displays web server SSL certificate details
	`->show ssl-certificate *` Displays detailed SSL certificate information

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@IPv4Address/ [filename]>`
	-or-
	`save ssl-csr address=<ftp://user:password@ipaddress> filename=<name>`

Item	Description
Properties	
`Address (required)`	A valid IPv4 address or host name of the FTP server, with user name, password, and name of the file to which the generated SSL CSR will be stored on the FTP server. If not specified, the default file name is "vc-ssl.csr".
`Filename (optional)`	The name of the file to which the generated SSL CSR will be stored on the FTP server. The filename can also be mentioned separately. If not specified, the default filename will be "vc-ssl.csr". The file path given will be treated as relative to the login directory for the user on the FTP server. The user should ensure that the permissions are appropriate for the transfer to succeed.
Examples	
	`->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/new-ssl.csr` Generates and transfers an SSL CSR and saves with a new filename
	`->save ssl-csr address=ftp://user:password@192.168.10.12 filename=new-ssl.csr` Generates and transfers an SSL CSR and saves 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	

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

In addition to the standard statistics, Virtual Connect also provides additional information on DCBX. DCBX is the data center discovery and capability exchange protocol used by DCB devices to exchange configuration information with directly-connected peers. The protocol can also be used for misconfiguration detection and for configuration of the peer. In this release, the VC module adopts the DCBX specification to implement the control state machine and three feature state machines:

- Priority Group (PG)
- Priority-based Flow Control (PFC)
- Application Protocol (AP)

The following tables lists the type of DCBX statistics displayed.

Item	Description
DCBX Application Protocol State	<enabled or disabled>
DCBX Overall Status	<OK, Failed, Unknown>
DCBX Pending Status	<false, true, or negotiating in progress>
DCBX Priority Flow Control State	<Status>
DCBX Priority Group State	<Status>
DCBX Application Protocol State	<Status>

The following table defines each statistic.

Item	Description
disabled	The feature is operationally disabled.
ok	The feature is configured properly or DCBX negotiation is in progress.
incompatible cnfg	A FlexFabric network adapter has an incompatible configuration and is not accepting changes.
peer_disabled	A FlexFabric network adapter reports that the feature is not enabled.
Does not support dcbx	A FlexFabric network adapter does not indicate that it supports the feature.

Item	Description
Not advertising dcbx support	A FlexFabric network adapter is not running DCBX within the expired period.
Error during cnfg	A FlexFabric network adapter reported an error configuring the feature.
Not accepting changes	A FlexFabric network adapter reported an error configuring the feature.

statistics-throughput

Manage the port throughput statistics.

Supported actions: `help, show, set`

Item	Description
`show statistics-throughput`	Display throughput information for the specified port.
Syntax	`show statistics-throughput <PortID>`
Parameter	
`PortID (required)`	The port ID of the port for which to display throughput information. PortID is composed of `<EnclosureID>:<BayNumber>:<PortLabel>`. Port throughput collection must be enabled for the domain by issuing the `set statistics-throughput` command. A column that contains an "R" indicates that the statistics were reset by the user during that time period, therefore the throughput is not available.
Example	
	`->show statistics-throughput enc0:1:X1` Displays the port throughput statistics for port X1 of the module in bay1 of enclosure enc0

Item	Description
`set statistics-throughput`	Enable or disable the port throughput statistics.
Syntax	`set statistics-throughput <Enabled=[true|false]>`
Parameter	
`Enabled (required)`	Enables or disables port throughput statistics. Valid values include "true" and "false". Port throughput statistics are accessible using the `show statistics-throughput` command.
Example	
	`->set statistics-throughput Enabled=true` Enables the port throughput statistics

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

storage-management

Manage iSCSI storage management information for LeftHand network P4000 devices.

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

Item	Description
`add storage-management`	Add iSCSI storage management credentials.
Syntax	`add storage-management <name> ip=<IPv4Address> username=<user_name> [password=<password>]`
Parameter	
`name (required)`	The name for the iSCSI storage management
Properties	
`ip (required)`	The iSCSI storage management IPv4 address
`username (required)`	An administrator for the storage management
`password (optional)`	The user password. The password can be entered as clear text in the command. If you do not specify the password, you are prompted to enter the password as a masked string at the prompt.
Examples	
	`->add storage-management SMName ip=16.89.125.10 username=user1 password=pass1` Adds iSCSI storage management records with password entered as clear text
	`->add storage-management SMName ip=16.89.125.12 username=user2` Add iSCSI storage management credential with password prompted and entered as a masked string

Item	Description
`remove storage-management`	Delete iSCSI storage management credential records.
Syntax	`remove storage-management [<name>|*]`
Parameter	
`name (required)`	The name of the storage management information being removed. Use "*" to remove all storage management records.
Examples	
	`->remove storage-management SMName` Removes the specified storage management records
	`->remove storage-management *` Removes all storage management records in the domain

Item	Description
`set storage-management`	Modify the specified iSCSI storage management credential.
Syntax	`set storage-management <name> [ip=<IPv4Address>] [username=<user_name>] [password=[<password>]]`
Parameter	
`name (required)`	The name for the iSCSI storage management
Properties	
`ip (optional)`	The iSCSI storage management IPv4 address

Item	Description
username (optional)	An administrator for the storage management
password (optional)	The user password. The password can be entered as clear text in the command. If you specify the password property without a value, you are prompted to enter the password as a masked string at the prompt.
Examples	
	->set storage-management SMName password=MyPassword Modifies iSCSI storage management records password with clear text
	->set storage-management SMName password= Modifies iSCSI storage management credential password (You will be prompted to enter password as a masked string.)

Item	Description
show storage-management	Displays storage management information (excluding passwords) in the domain.
Syntax	show storage-management [<name>|*]
Parameter	
name (optional)	The name of the existing storage management information in the domain. Use "*" to display detailed information for all storage management records. If no value is specified, a summary of all storage management records appears.
Example	
	->show storage-management Displays summary information for all storage management records
	->show storage-management SMName Displays details on the specified storage management records
	->show storage-management * Displays details on all storage management records in the domain

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/[filename] | ftp://user:password@ipaddress>/[filename]
Property	
address (required)	A valid IPv4 address of a TFTP or FTP server, with user name, password (where required), and name of the file to which the generated support info will be stored on the FTP server. If not specified, the default file name is "vc-support-info".
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`	Displays the last `n` records. If this option is specified and no value is provided, the last 10 records are displayed.
`First`	Displays the first `n` records. If this option is specified and no value is provided, the first 10 records are displayed.
`Pause`	The number of records to be viewed before prompting for a 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 50)."

tacacs

Manage TACACS+ authentication settings.

Supported actions: `help, set, show`

Item	Description
`set tacacs`	Modify and test the Virtual Connect TACACS+ authentication settings.
Syntax	`set tacacs [-test] [Enabled=<true|false>] [ServerAddress=<IP Address|DNS Name>] [Port=<portNum>] [ServerKey=<key>] [Timeout=<timeout>] [SecondaryServerAddress=<IP Address|DNS Name>] [SecondaryPort=<portNum>] [SecondaryServerKey=<key>] [SecondaryTimeout=<timeout>] [LoggingEnabled=<true|false>]`
Option	
`Test (optional)`	Tests the TACACS+ configuration without applying changes
Properties	
`Enabled (optional)`	Enables or disables TACACS+ authentication. Valid values include "true" and "false".
`ServerAddress (optional)`	The IP address or the DNS name of the primary TACACS+ server used for authentication

Item	Description
`Port (optional)`	The server TCP port number. Valid values include a valid port number between 1 and 65535. The default port number is 49.
`ServerKey (optional)`	The plain-text string used to encrypt user details exchanged with the primary TACACS server. It must match the server key configured for this VC on the primary server. TACACS authentication will not work if the server key is blank or null.
`Timeout (optional)`	The time in seconds by which a server response must be received before a new request is made. The valid range of values is from 1 to 600 seconds. The default timeout is 10 seconds.
`SecondaryServer Address (optional)`	The IP address or host name of the secondary TACACS server used for authentication
`SecondaryPort (optional)`	The TCP port to use for TACACS communication. Valid values include a valid port number between 1 and 65535. The default TCP port number is 49.
`SecondaryServerKey (optional)`	The plain-text string used to encrypt user details exchanged with the secondary TACACS server. It must match the server key configured for this VC on the secondary server. TACACS authentication will not work if the server key is blank or null.
`SecondaryTimeout (optional)`	The timeout value in seconds for TACACS communication with the secondary server
`LoggingEnabled (optional)`	Enables or disables command logging on the TACACS+ server. Valid values include "true" and "false".
Examples	
	`->set tacacs -test Enabled=true ServerAddress=192.168.0.27` Tests the TACACS+ configuration changes without applying them
	`->set tacacs Enabled=true ServerAddress=192.168.0.124 ServerKey=test123 SecondaryServerAddress=tacserver.hp.com SecondaryServerKey=test456` Enables TACACS+ authentication for users
	`->set tacacs LoggingEnabled=true` Enables TACACS server logging

Item	Description
`show tacacs`	Display the Virtual Connect TACACS+ authentication settings.
Syntax	`show tacacs`
Example	
	`->show tacacs` Displays TACACS+ information

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>]`

Item	Description
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 shared uplink set name is not specified
UplinkSet (required)	The name of an existing shared uplink set to which the port is added if the network name is not 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 port speed is "Auto". If no connector is present on the uplink port, only "Auto" and "Disabled" can be configured as the 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". Valid values include "Primary" and "Secondary". The default is "Primary".
Examples	
	->add uplinkport enc0:1:1 Network=MyNetwork Adds a new uplink port (Bay 1, Port 1) to a network named MyNetwork
	->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 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 removed
UplinkSet (optional)	The name of the shared uplink set from which the port is removed
Examples	
	->remove uplinkport enc0:1:2 Network=MyNetwork Removes a specific uplink port (Bay 1, Port 2) from a network named MyNetwork
	->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.

Item	Description
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 shared uplink set. The port ID is in the format `<EnclosureID>:<BayNumber>:<PortNumber>`.
Properties	
`Network (required)`	The name of the network to which the port belongs if the shared uplink set name is not specified
`UplinkSet (required)`	The name of the shared uplink set to which the port belongs if the network name is not specified
`Speed (optional)`	Specifies the port speed for the port. Valid values include "Auto", "10Mb", "100Mb", "1Gb", "10Gb", and "Disabled". If no connector is present on the uplink port, only "Auto" and "Disabled" can be configured as the 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". Valid values are "Primary" and "Secondary". 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 Secondary 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 set, it appears. If the port is unlinked and no connectivity exists, the cause is displayed. For more information about possible causes, see "Port status conditions (on page 148)."
Syntax	`show uplinkport <PortID|*> [FilterBy]`
Parameters	
`PortID (optional)`	The ID of an uplink port. The PortID format is `<EnclosureID>:<Bay>:<PortNumber>`. Use "*" to display 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, specify `ID=enc0`. To display all ports using an RJ-45 connector type, specify `Type=RJ45`. You can specify more than one filter option in 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

Item	Description
	->show uplinkport * Displays all uplink ports in the enclosure (detailed view)
	->show uplinkport ID=enc0:1 Displays all the uplink ports for bay 1 of the local enclosure
	->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 bay 1 of the local enclosure with connector type RJ-45

uplinkset

Manage shared uplink sets.

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

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

Item	Description
copy uplinkset	Copy a shared uplink port set.
Syntax	copy uplinkset <fromSUS> <toSUS> fromVlanStr=<vlanString> toVlanStr=<vlanString> [replace=<all|first|last>]
Parameters	
fromSUS (required)	The unique name of the shared uplink set to copy from
toSUS (required)	The unique name of the shared uplink set to copy to
Properties	
fromVlanStr (required)	The partial network name string to be replaced. The fromVlanStr property cannot be empty and must be existing in all associated network names.
toVlanStr (required)	The network name string to be replaced to. The new network name cannot exceed 64 characters. This string can be empty, which is considered as removing fromVlanStr from all associated network names.
replace (optional)	The instance of the string replacement to occur. Valid values include "all", "first", and "last". The default value is "all".
Example	
	->copy uplinkset uplinkset_1 uplinkset_2 fromVlanStr=LEFT toVlanStr=RIGHT replace=first

Item	Description
	Copies uplinkset_1 to uplinkset_2 and replaces the first instance of LEFT to RIGHT in the name string of all associate networks

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 set. Use "*" to remove all existing shared uplink sets from the domain.
Example	
	`->remove uplinkset MyUplinkSet` Removes a shared uplink set
	`->remove uplinkset *` Removes all shared uplink sets from the domain

Item	Description
`set uplinkset`	Modify an existing shared uplink port set.
Syntax	`set uplinkset <UplinkSetName> [Name=<NewName>] [ConnectionMode=<Auto|Failover>]`
Parameter	
`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 shared uplink set. Valid values include "Auto" and "Failover". The default value is "Auto".
Examples	
	`->set uplinkset Blue Name=Red` Changes the name of a shared uplink set from Blue to Red
	`->set uplinkset Blue connectionMode=Failover` Changes the connection mode of a shared uplink set named Blue to Failover

Item	Description
`show uplinkset`	Display shared uplink configurations.
Syntax	`show uplinkset [<UplinkSetName> | *]`
Parameter	
`UplinkSetName (optional)`	Name of an existing shared uplink set. Use "*" to display a detailed view of all shared uplink sets. If not specified, a summary of all shared uplink sets is displayed.
Examples	
	`->show uplinkset` Displays a summary of all shared uplink sets
	`->show uplinkset *` Displays detailed information for all shared uplink sets
	`->show uplinkset MyUplinkSet` Displays detailed information for a shared uplink set named MyUplinkSet

user

Manage local domain user configurations.

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

Item	Description
`add user`	Create a new user and add the user 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 user name must be unique within the domain.
Properties	
`Password (required)`	The password for the new user. The new user password 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, the default is "true".
`Privileges (optional)`	The allowed privileges for the user. The privileges can be any combination of "domain", "server", "network", or "storage" separated by commas. If no privileges are specified, the user can view domain information only. Use "*" to specify all privileges.
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 to be removed. Use "*" to remove all users except for the default Administrator account.
Examples	
	`->remove user steve` Removes a specific user by name
	`->remove user *` Removes all users except the default Administrator account

Item	Description
`set user`	Modify attributes of an existing user.
Syntax	`set user <UserName> [<password>] [FullName=<Full Name>] [ContactInfo=<Contact Details>] [Enabled=<True|False>]`

Item	Description
	`[Privileges=<Storage|Network|Server|Domain|*>]`
Parameter	
`UserName (required)`	The name of the user to modify
Properties	
`Password (optional)`	The new password of the user can be entered as clear text in the command. If the Password value is blank, you are prompted to enter the password, and the characters entered are masked.
`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". The default value is "true".
`Privileges (optional)`	The allowed privileges for the user. The privileges can be any combination of "domain", "server", "network", or "storage" separated by commas. If no privileges are specified, the user can view domain information only. Use "*" to specify all privileges.
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, a summary of all users is displayed. Use "*" to display detailed information for all users.
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

Item	Description
	for user passwords.
Syntax	`set user-security [StrongPasswords=<Enabled|Disabled>] [MinPasswordLength=<3-40>]`
Properties	
`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 backup VCM can also be specified (optional), if a backup VCM is available. **IMPORTANT:** Resetting the VCM causes a temporary loss in connectivity with the Virtual Connect Manager. If failover is specified and a backup VCM exists, users are logged off and must reconnect using the backup VCM IP address.
Syntax	`reset vcm [-failover]`
Option	
`Failover`	Forces a failover from the current primary VCM to the backup VCM.
Examples	
	`->reset vcm` Resets the Virtual Connect Manager
	`->reset vcm -failover` Resets the Virtual Connect Manager and forces a failover to the backup VCM (if available)

User privileges

The following table lists required user privileges for CLI commands.

Command	Element	Domain	Network	Server	Storage	All access
add	banner	X	—	—	—	—
	enet-connection	—	—	X	—	—
	fabric	—	—	—	X	—
	fc-connection	—	—	X	—	—
	fcoe-connection	—	—	X	—	—
	interconnect	X	—	—	—	—
	isci-connection	—	—	X	—	—
	storage-management	—	—	—	X	—
	ldap-group	X	—	—	—	—
	radius-group	X	—	—	—	—
	log-target	X	—	—	—	—
	nag-network	—	X	—	—	—
	network	—	X	—	—	—
	network-access-group	—	X	—	—	—
	port-monitor	—	X	X	—	—
	profile	—	—	X	—	—
	server-port-map	—	—	X	—	—
	snmp-trap	X	X	—	—	—
	uplinkport	—	X	—	—	—
	uplinkset	—	X	—	—	—
	user	X	—	—	—	—
assign	profile	—	—	X	—	—
copy	profile	—	—	X	—	—
delete	domain	X	—	—	—	—
exit	—	X	X	X	X	X
help	—	X	X	X	X	X
import	enclosure	X	—	—	—	—
load	ldap-certificate	X	—	—	—	—
	profile	X	—	—	—	—
	ssh	X	—	—	—	—
	ssl-certificate	X	—	—	—	—
poweroff	server	—	—	X	—	—
poweron	server	—	—	X	—	—
reboot	server	—	—	X	—	—

Command	Element	Domain	Network	Server	Storage	All access
remove	banner	X	—	—	—	—
	enclosure	X	—	—	—	—
	enet-connection	—	—	X	—	—
	external-manager	X	—	—	—	—
	fabric	—	—	—	X	—
	fc-connection	—	—	X	—	—
	fcoe-connection	—	—	X	—	—
	interconnect	X	—	—	—	—
	iscsi-boot-param	—	—	X	—	—
	iscsi-connection	—	—	X	—	—
	storage-management	—	—	—	X	—
	ldap-certificate	X	—	—	—	—
	ldap-group	X	—	—	—	—
	radius-group	X	—	—	—	—
	log-target	X	—	—	—	—
	nag-network	—	X	—	—	—
	network	—	X	—	—	—
	network-access-group	—	X	—	—	—
	port-monitor	—	X	X	—	—
	profile	—	—	X	—	—
	server-port-map	—	—	X	—	—
	snmp-trap	X	X	—	—	—
	ssh	X	—	—	—	—
	uplinkport	—	X	—	—	—
	uplinkset	—	X	—	—	—
	user	X	—	—	—	—
reset	loop-protect	—	X	—	—	—
	statistics	—	X	—	—	—
	vcm	X	—	—	—	—
save	configbackup	X	—	—	—	—
	profile	—	—	X	—	—
	ssl-csr	X	—	—	—	—
	supportinfo	X	X	X	X	X
set	configuration	X	—	—	—	—
	domain	X	—	—	—	—

Command	Element	Domain	Network	Server	Storage	All access
	enet-connection	—	—	X	—	—
	enet-vlan	—	X	—	—	—
	external-manager	X	—	—	—	—
	fabric	—	—	—	X	—
	fc-connection	—	—	X	—	—
	fcoe-connection	—	—	X	—	—
	igmp	—	X	—	—	—
	interconnect	X	—	—	—	—
	iscsi-boot-param	—	—	X	—	—
	iscsi-connection	—	—	X	—	—
	storage-management	—	—	—	X	—
	ldap	X	—	—	—	—
	ldap-group	X	—	—	—	—
	radius	X	—	—	—	—
	radius-group	X	—	—	—	—
	tacacs	X	—	—	—	—
	role	X	—	—	—	—
	link-dist-interval	—	—	—	X	—
	log-target	X	—	—	—	—
	loop-protect	—	X	—	—	—
	mac-cache	—	X	—	—	—
	network	—	X	—	—	—
	network-access-group	—	X	—	—	—
	port-monitor	—	X	X	—	—
	profile	—	—	X	—	—
	serverid	—	—	X	—	——
	server-port-map	—	—	X		—
	snmp	X	X	—	—	—
	snmp-trap	X	X	—	—	—
	ssl	X	—	—	—	—
	statistics-throughput	—	X	—	—	—
	uplinkport	—	X	—	—	—
	uplinkset	—	X	—	—	—
	user	X	—	—	—	—
	user-security	X	—	—	—	—

Command	Element	Domain	Network	Server	Storage	All access
show	all	X	X	X	X	X
	banner	X	X	X	X	X
	configuration	X	—	—	—	—
	devicebay	X	X	X	X	X
	domain	X	X	X	X	X
	enclosure	X	X	X	X	X
	enet-connection	X	X	X	X	X
	enet-vlan	X	X	X	X	X
	external-manager	X	X	X	X	X
	fabric	X	X	X	X	X
	fc-connection	X	X	X	X	X
	fcoe-connection	X	X	X	X	X
	firmware	X	X	X	X	X
	igmp	X	X	X	X	X
	igmp-group	X	X	X	X	X
	interconnect	X	X	X	X	X
	interconnect-mac-table	X	X	X	X	X
	iscsi-boot-param	X	X	X	X	X
	iscsi-connection	X	X	X	X	X
	storage-management	X	X	X	X	X
	ldap	X	X	X	X	X
	ldap-certificate	X	X	X	X	X
	ldap-group	X	X	X	X	X
	radius	X	X	X	X	X
	radius-group	X	X	X	X	X
	tacacs	X	X	X	X	X
	role	X	X	X	X	X
	link-dist-interval	X	X	X	X	X
	lldp	X	X	X	X	X
	log-target	X	X	X	X	X
	loop-protect	X	X	X	X	X
	mac-cache	X	X	X	X	X
	nag-network	X	X	X	X	X
	network	X	X	X	X	X
	network-access-group	X	X	X	X	X

Command	Element	Domain	Network	Server	Storage	All access
	port-monitor	X	X	X	X	X
	profile	X	X	X	X	X
	config	X	—	—	—	—
	server	X	X	X	X	X
	serverid	X	X	X	X	X
	server-port	X	X	X	X	X
	server-port-map	X	X	X	X	X
	snmp	X	X	X	X	X
	snmp-trap	X	X	X	X	X
	ssh	X	X	X	X	X
	ssl	X	X	X	X	X
	ssl-certificate	X	X	X	X	X
	stackinglink	X	X	X	X	X
	statistics	X	X	X	X	X
	statistics-throughput	X	X	X	X	X
	status	X	X	X	X	X
	systemlog	X	—	—	—	—
	uplinkport	X	X	X	X	X
	uplinkset	X	X	X	X	X
	user	X	—	—	—	—
	user-security	X	X	X	X	X
	version	X	X	X	X	X
test	log-target	X	X	X	X	X
	snmp-trap	X	X	X	X	X
unassign	profile	—	—	X	—	—

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, you 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.

When scripting CLI commands, only a single scripting client should perform remote management operations to a remote VC Manager. If multiple scripting clients are used to perform a heavy load of CLI commands to a single VC Manager, some management commands might fail. In some cases, the primary module might need to be reset to recover properly.

- **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 discarded to prevent delivery to a higher-layer protocol even though no errors were detected. These packets can be discarded to make buffer space available.
rfc1213_IfInErrors	1213	The number of inbound packets containing errors that prevent delivery to a higher-layer protocol
rfc1213_IfInNUcastPkts	1213	The total number of packets that higher-level protocols requested to be transmitted to a nonunicast address (such as a subnetwork-broadcast address or a subnetwork-multicast address), including those packets 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_IfInUnknown Protos	1213	The number of packets received through the interface that were discarded due to an unknown or unsupported protocol
rfc1213_IfOutDiscards	1213	The number of outbound packets discarded to prevent transmission even though no errors were detected. These packets can be discarded to make buffer space available.
rfc1213_IOutErrors	1213	The number of outbound packets that could not be transmitted due to errors
rfc1213_IfOutNUcastPkts	1213	The total number of packets that higher-level protocols requested to be transmitted to a subnetwork-unicast address, including those packets that were discarded or not sent
rfc1213_IfOutOctets	1213	The total number of octets transmitted through 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 to be transmitted to a subnetwork-unicast address, including those packets that were discarded or not sent
rfc1213_IpForwDatagrams	1213	The number of input datagrams for which this entity was not the final IP destination, resulting in an attempt being made to locate a route to the final destination. In entities that do not act as IP gateways, this counter only includes packets that were source-routed through this entity with successful source-route option processing.
rfc1213_IpInDiscards	1213	The number of input datagrams discarded to prevent continued processing even though no problems were encountered. These datagrams can be discarded to make buffer space available. This counter does not include any datagrams discarded while awaiting reassembly.

Name	RFC	Description
rfc1213_IpInHdrErrors	1213	The number of input datagrams discarded due to errors in the IP header. Possible errors include bad checksums, version number mismatches, format errors, time-to-live exceeded, errors discovered while processing IP options, and so on.
rfc1213_IpInReceives	1213	The total number of input datagrams received from interfaces, including datagrams received in error
rfc1493_Dot1dBasePort DelayExceededDiscards	1493	The number of frames discarded by this port due to an excessive transit delay through the bridge (incremented by both transparent and source route bridges)
rfc1213_Dot1dBasePort MtuExceededDiscards	1493	The number of frames discarded by this port due to excessive size (incremented by both transparent and source route bridges)
rfc1213_Dot1dPortIn Discards	1493	The number of valid frames received that were discarded (filtered) by the Forwarding Process
rfc1213_Dot1dTpPortIn Frames	1493	The number of frames received by this port from its segment. A frame received on the interface that corresponds to this port is only counted by this object if it is for a protocol being processed by the local bridging function, including bridge management frames.
rfc1757_StatsBroadcast Pkts	1757	The number of good packets received during the sampling interval that were directed to the broadcast address
rfc1757_StatsCRCAlign Errors	1757	The total number of packets received with a length of between 64 and 1518 octets (excluding framing bits, but including FCS octets), inclusive, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
rfc1757_StatsCollisions	1757	The best estimate of the total number of collisions in this Ethernet segment. The value returned depends 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. Therefore, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment. Probe location plays a smaller role for 10BASE-T. Section 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. Therefore, probes placed on a station and a repeater should report the same number of collisions. 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 a lack of resources. This represents the number of times the condition was detected, which does not necessarily equal the number of dropped packets.

Name	RFC	Description
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 FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). It is entirely normal for etherStatsFragments to increment, 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 FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). 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. 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. For greater precision, sample the etherStatsPkts and etherStatsOctets objects 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: Utilization = [Pkts * (9.6 + 6.4) + (Octets * .8)] / 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
rfc1757_StatsPkts1024to 1518Octets	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_StatsPkts128to 255Octets	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_StatsPkts256to 511Octets	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_StatsPkts512to 1023Octets	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)

Name	RFC	Description
rfc1757_StatsPkts65to 127Octets	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, not including oversized packets
rfc1757_StatsUndersize Pkts	1757	The number of packets received during the sampling interval that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed
rfc2233_IfHCInBroadcast Pkts	2233	The number of packets, delivered by this sublayer to a higher sublayer, that were addressed to a broadcast address at this sublayer. This object is a 64-bit version of ifInBroadcastPkts. Discontinuities in the value of this counter can occur at reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCInMulticast Pkts	2233	The number of packets, delivered by this sublayer to a higher sublayer, that were addressed to a multicast address at this sublayer. 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 reinitialization 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 reinitialization 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 to be transmitted but were not addressed to a multicast or broadcast address at this sublayer, including those packets 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCOut BroadcastPkts	2233	The total number of packets that higher-level protocols requested to be transmitted that were addressed to a broadcast address at this sublayer, including those packets 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2233_IfHCOutMulticast Pkts	2233	The total number of packets that higher-level protocols requested to be transmitted that were addressed to a multicast address at this sublayer, including those packets 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 reinitialization 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.

Name	RFC	Description
rfc2233_IfHCOutUcastPkts	2233	The total number of packets that higher-level protocols requested to be transmitted but were not addressed to a multicast or broadcast address at this sublayer, including those packets 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3ControlIn UnknownOpcodes	2665	The number of MAC Control frames received on the interface that contain an opcode that is not supported by the device. Discontinuities in the value of this counter can occur at reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3InPause Frames	2665	The number of MAC Control frames received on the 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3OutPause Frames	2665	The number of MAC Control frames transmitted on the 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3Stats AlignmentErrors	2665	The number 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 with multiple error conditions are counted exclusively according to the error status presented to the LLC, per the conventions of IEEE 802.3 Layer Management. This counter does not increment for 8-bit wide group encoding schemes. Discontinuities in the value of this counter can occur at reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsCarrier SenseErrors	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 by an instance of this object is incremented once per transmission attempt at most, 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3Stats DeferredTransmissions	2665	The number 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.

Name	RFC	Description
rfc2665_Dot3Stats ExcessiveCollisions	2665	The number 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsFCS Errors	2665	The number 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 a 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 with multiple error conditions are counted exclusively according to the error status presented to the LLC, per the conventions of IEEE 802.3 Layer Management. Coding errors detected by the physical layer for speeds above 10 Mb/s cause the frame to fail the FCS check. Discontinuities in the value of this counter can occur at reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsFrame TooLongs	2665	The number 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 with multiple error conditions are counted exclusively according to the error status presented to the LLC, per the conventions of IEEE 802.3 Layer Management. Discontinuities in the value of this counter can occur at reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsInternal MacReceiveErrors	2665	The number 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. An instance of this object can represent a count of receive errors on a particular interface that are not otherwise counted. Discontinuities in the value of this counter can occur at reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsInternal MacTransmitErrors	2665	The number 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. An instance of this object can 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.

Name	RFC	Description
rfc2665_Dot3StatsLate Collisions	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 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsSQE TestErrors	2665	The number 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime. The object type is dot3StatsSQETestErrors.
rfc2665_Dot3StatsSingle CollisionFrames	2665	The number 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 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.
rfc2665_Dot3StatsSymbol Errors	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 occurrence of an event that caused 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 caused the PHY to indicate 'Data reception error' on the GMII. The count represented by an instance of this object is incremented once per carrier event at most, 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 reinitialization of the management system and at other times as indicated by the value of ifCounterDiscontinuityTime.

FCoE downlink ports

Name	RFC	Description
fcAddressErrors	4044	The number of frames received with unknown addressing, such as an unknown SID or DID. The object type is fcmPortAddressErrors.

Name	RFC	Description
fcBBCreditFrameFailures	N/A	The number of times that 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	The number of Class 2 frames received at this port. The object type is fcmPortClass2RxFrames.
fcClass2TxFrames	4044	The number of Class 2 frames transmitted out of this port. The object type is fcmPortClass2TxFrames.
fcClass3Discards	4044	The number of Class 3 frames that were discarded upon reception at this port. The object type is fcmPortClass3Discards.
fcClass3RxFrames	4044	The number of Class 3 frames received at this port. The object type is fcmPortClass3RxFrames.
fcClass3TxFrames	4044	The number of Class 3 frames transmitted out of this port. The object type is fcmPortClass3TxFrames.
fcDecodeErrors	N/A	The number of errors that occurred while converting the incoming 10-bit data stream into 8-bit data for processing. An increasing value of this counter indicates a potential hardware problem between the module and the FC mezzanine SerDes settings.
fcFBSYFrames	4044	The number of times that FBSY 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. This counter does not increment for an F_Port. The object type is fcmPortClass2RxFbsyFrames.
fcFRJTFrames	4044	The number of times that FRJT was returned to this port as a result of a Class 2 frame being rejected by the fabric. This counter does not increment for an F_Port. The object type is fcmPortClass2RxFrjtFrames.
fcFramesTooLong	4044	The number of frames received at this port for which the frame length was greater than what was agreed to in FLOGI/PLOGI. This can be caused by losing the end of frame delimiter. The object type is fcmPortFrameTooLongs.
fcFramesTruncated	4044	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 that an optional header should have been present. The object type is fcmPortTruncatedFrames.
fcInvalidCRC	4044	The number of frames received with an invalid CRC. This count is part of FC-PH's Link Error Status Block (LESB). The object type is fcmPortInvalidCRCs.
fcInvalidTxWords	4044	The number of invalid transmission words received at this port. This count is part of FC-PH's LESB. The object type is fcmPortInvalidTxWords.
fcLinkFailures	4044	The number of link failures. This count is part of FC-PH's LESB. The object type is fcmPortLinkFailures.
fcLossOfSynchronization	4044	The number of instances of synchronization loss detected at this port. This count is part of FC-PH's LESB. The object type is fcmPortLossofSynchs.
fcNumberLinkResets	4044	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. The object type is fcmPortLinkResets.

Name	RFC	Description
fcNumberOffline Sequences	FCMGMT-MIB	The number of Offline Primitive sequence received at this port. This statistic is for Fibre Channel only. The object type is connUnitPortStatCountNumberOfflineSequences.
fcPrimitiveSeqProtocol Errors	4044	The number of primitive sequence protocol errors detected at this port. This count is part of FC-PH's LESB. The object type is fcmPortPrimSeqProtocolErrors.
fcRxByteRate	N/A	The average receive byte rate (byte/s) for a sample period of once per second
fcRxFrameRate	N/A	The average receive frame rate (frame/s) for a sample period of once per second
fcRxLinkResets	4044	The number of Link Reset (LR) Primitive Sequences received. The object type is fcmPortRxLinkResets.
fcRxOfflineSequences	4044	The number of Offline (OLS) Primitive Sequences received at this port. The object type is fcmPortRxOfflineSequences.
fcSmoothingOverflow Errors	N/A	The number of times that a violation of FC rules on the incoming signal were detected. An example of a violation is an insufficient number of idles received between the frames.
fcTotalRxBytes	N/A	The total number of bytes received
fcTotalRxFrames	N/A	The total number of frames received
fcTotalTxBytes	N/A	The total number of bytes transmitted
fcTotalTxFrames	N/A	The total number of frames transmitted
fcTxByteRate	N/A	The average transmit byte rate (byte/s) for a sample period of once per second
fcTxFrameRate	N/A	The average transmit frame rate (frame/s) for a sample period of once per second
fcTxLinkResets	4044	The number of LR Primitive Sequences transmitted. The object type is fcmPortTxLinkResets.
fcTxOfflineSequences	4044	The number of OLS Primitive Sequences transmitted by this port. The object type is fcmPortTxOfflineSequences.

FC uplink ports

Name	RFC	Description
numAddressErrors	FCMGMT-MIB	The number of frames received with unknown addressing, such as an unknown SID or DID. The SID or DID is not known to the routing algorithm. The object type is connUnitPortStatCountAddressErrors.
numBBCreditZero	FCMGMT-MIB	The number of transitions in or out of the BBcredit zero state. The other side does not provide any credit. The object type is connUnitPortStatCountBBCreditZero.
numBytesRx	N/A	The total number of bytes received
numBytesTx	N/A	The total number of bytes transmitted
numCRCErrors	FCMGMT-MIB	The number of frames received with invalid CRC. This count is part of FC-PH's LESB. Loop ports should not count CRC errors passing through when monitoring. The object type is connUnitPortStatCountInvalidCRC.
numClass3Discards	FCMGMT-MIB	The number of Class 3 frames discarded upon reception at this port. No FBSY or FRJT is generated for Class 3 frames, and they are discarded if they cannot be delivered. The object type is connUnitPortStatCountClass3Discards.

Name	RFC	Description
numEncodingDisparity Errors	FCMGMT -MIB	The number of disparity errors received at this port. The object type is connUnitPortStatCountEncodingDisparityErrors.
numFBSYFrames	FCMGMT -MIB	The number of times that FBSY was returned to this port as a result of a frame that could not be delivered to the other end of the link. This occurs on SOFc1 frames (the frames that establish a connection) if either the fabric or the destination port is temporarily busy. The count is the sum of all classes. The object type is connUnitPortStatCountFBSYFrames.
numFRJTFrames	FCMGMT -MIB	The number of times that FRJT was returned to this port as a result of a frame being rejected by the fabric. This count is the total for all classes. The object type is connUnitPortStatCountFRJTFrames.
numFramesTooLong	FCMGMT -MIB	The number 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. The object type is connUnitPortStatCountFramesTooLong.
numInputBuffersFull	FCMGMT -MIB	The number of times that 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. The object type is connUnitPortStatCountInputBuffersFull.
numInvalidOrderedSets	FCMGMT -MIB	The number of invalid ordered sets received at port. This count is part of FC-PH's LESB. The object type is connUnitPortStatCountInvalidOrderedSets.
numInvalidTransmission Words	FCMGMT -MIB	The number of invalid transmission words received at this port. This count is part of FC-PH's LESB. The object type is connUnitPortStatCountInvalidTxWords.
numLRsRx	FCMGMT -MIB	The number of LRs received. This statistic is for Fibre Channel only. The object type is connUnitPortStatCountRxLinkResets.
numLRsTx	FCMGMT -MIB	The number of LRs transmitted. The object type is connUnitPortStatCountTxLinkResets.
numLinkFailures	FCMGMT -MIB	The number of link failures. This count is part of FC-PH's LESB. The object type is connUnitPortStatCountLinkFailures.
numLossOfSignal	FCMGMT -MIB	The number of instances of signal loss detected at this port. This count is part of FC-PH's LESB. The object type is connUnitPortStatCountLossofSignal.
numLossOfSync	FCMGMT -MIB	The number of instances of synchronization loss detected at this port. This count is part of FC-PH's LESB. The object type is connUnitPortStatCountLossofSynchronization.
numMcastFramesRx	FCMGMT -MIB	The number of multicast frames or packets received at this port. The object type is connUnitPortStatCountRxMulticastObjects.
numMcastFramesTx	FCMGMT -MIB	The number of multicast frames or packets transmitted through this port. The object type is connUnitPortStatCountTxMulticastObjects.
numMcastTimeouts	N/A	The number of timeouts reported for multicast frames. A single frame could cause this counter to increment if it timed out for each multiple destination.
numPrimitiveSeqProtocol Err	FCMGMT -MIB	The number of primitive sequence protocol errors detected at this port. This count is part of FC-PH's LESB. The object type is connUnitPortStatCountPrimitiveSequenceProtocolErrors.
numRxBadEOFs	N/A	The number of frames received with a badly formed end-of-frame
numRxCRCs	N/A	The number of CRC errors detected in received frames

Name	RFC	Description
numRxClass1Frames	FCMGMT-MIB	The number Class 1 frames received at this port. This statistic is for Fibre Channel only. The object type is connUnitPortStatCountClass1RxFrames.
numRxClass2Frames	FCMGMT-MIB	The number of Class 2 frames received at this port. The object type is connUnitPortStatCountClass2RxFrames.
numRxClass3Frames	FCMGMT-MIB	The number of Class 3 frames received at this port. The object type is connUnitPortStatCountClass3RxFrames.
numRxLCs	N/A	The number of link control frames received at this port
numRxOfflineSequences	FCMGMT-MIB	The number of Offline Primitive OLSs received at this port. The object type is connUnitPortStatCountRxOfflineSequences.
rxBytePeakRate	N/A	The receive max byte rate since the last reset (bytes/s)
rxByteRate	N/A	The receive instantaneous byte rate (bytes/s)
rxFramePeakRate	N/A	The receive max frame rate since the last reset (frames/s)
rxFrameRate	N/A	The receive instantaneous frame rate (frames/s)
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	The SFP status
txBytePeakRate	N/A	The transmission max byte rate since the last reset (bytes/s)
txByteRate	N/A	The receive instantaneous byte rate (bytes/s)
txFramePeakRate	N/A	The transmission max frame rate since the last reset (frames/s)
txFrameRate	N/A	The transmission instantaneous frame rate (frames/s)

FC downlink ports

Statistics are not currently available for Fibre Channel downlink ports.

Fibre Channel modules

ADDRESSERRORS

Object type	connUnitPortStatCountAddressErrors
Description	The number of frames received with unknown addresses, such as an unknown SID or DID. The SID or DID is not known to the routing algorithm. ::= { connUnitPortStatEntry 48 }

BBCREDITZERO

Object type	connUnitPortStatCountBBCreditZero
Description	The number of transitions in or out of the BBcredit zero state. The other side does not provide any credit. ::= { connUnitPortStatEntry 8 }

BYTESRECEIVED

Object type	connUnitPortStatCountRxElements
Description	The number of octets or bytes received by this port in 1-second periodic polling of the port. This value is saved and compared with the next polled value to compute the net throughput. For Fibre Channel, ordered sets are not included in the count.

	::= { connUnitPortStatEntry 7 }

BYTESTRANSMITTED

Object type	connUnitPortStatCountTxElements
Description	The number of octets or bytes transmitted by this port in 1-second periodic polling of the port. This value is saved and compared with the next polled value to compute the net throughput. For Fibre Channel, ordered sets are not included in the count. ::= { connUnitPortStatEntry 6 }

CLASS3DISCARDS

Object type	connUnitPortStatCountClass3Discards
Description	The number of Class 3 frames discarded upon reception at this port. No FBSY or FRJT is generated for Class 3 frames, and they are discarded if they cannot be delivered. ::= { connUnitPortStatEntry 28 }

CRCERRORS

Object type	connUnitPortStatCountInvalidCRC
Description	The number of frames received with an invalid CRC. This count is part of FC-PH's LESB. Loop ports should not count CRC errors passing through when monitoring. ::= { connUnitPortStatEntry 40 }

DELIMITERERRORS

Object type	connUnitPortStatCountDelimiterErrors
Description	The number of invalid frame delimiters received at this port, for example, a frame with a class 2 at the start and a class 3 at the end. ::= { connUnitPortStatEntry 49 }

ENCODINGDISPARITYERRORS

Object type	connUnitPortStatCountEncodingDisparityErrors
Description	The number of disparity errors received at this port ::= { connUnitPortStatEntry 50 }

FBSYSFRAMES

Object type	connUnitPortStatCountFBSYFrames
Description	The number of times that FBSY was returned to this port as a result of a frame that could not be delivered to the other end of the link. This occurs on SOFc1 frames (the frames that establish a connection) if either the fabric or the destination port is temporarily busy. The count is the sum of all classes. If you cannot keep the counters by class, keep the sum counters. ::= { connUnitPortStatEntry 10 }

FRAMESRECEIVED

Object type	connUnitPortStatCountRxObjects
Description	The number of frames, packets, IOs, and so on received by this port. A Fibre Channel frame starts with SOF and ends with EOF. FC loop devices should not count frames passed through. This value represents the sum total for all other Rx objects. ::= { connUnitPortStatEntry 5 }

FRAMESTOOLONG

Object type	connUnitPortStatCountFramesTooLong
Description	The number 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. ::= { connUnitPortStatEntry 46 }

FRAMESTRANSMITTED

Object type	connUnitPortStatCountTxObjects
Description	The number of frames, packets, IOs, and so on that have been transmitted by this port. A Fibre Channel frame starts with SOF and ends with EOF. FC loop devices should not count frames passing through. This value represents the sum total for all other Tx objects. ::= { connUnitPortStatEntry 4 }

FRJTFRAMES

Object type	connUnitPortStatCountFRJTFrames
Description	The number of times that FRJT was returned to this port as a result of a frame being rejected by the fabric. The count is the total for all classes. ::= { connUnitPortStatEntry 12 }

INPUTBUFFERSFULL

Object type	connUnitPortStatCountInputBuffersFull
Description	The number of times that all input buffers of a port were full and the outbound buffer-to-buffer credit transitioned to zero. There is no credit to provide to the other side. ::= { connUnitPortStatEntry 9 }

INVALIDORDEREDSETS

Object type	connUnitPortStatCountInvalidOrderedSets
Description	The number of invalid ordered sets received at a port. This count is part of FC-PH's LESB. ::= { connUnitPortStatEntry 45 }

INVALIDTRANSMISSIONWORDS

Object type	connUnitPortStatCountInvalidTxWords
Description	The number of invalid transmission words received at this port. This number is part of FC-PH's LESB. ::= { connUnitPortStatEntry 41 }

LINKFAILURES

Object type	connUnitPortStatCountLinkFailures
Description	The number of link failures. This number is part of FC-PH's LESB. ::= { connUnitPortStatEntry 39 }

LINKRESETRECEIVED

Object type	connUnitPortStatCountRxLinkResets

Description	The number of LRs received ::= { connUnitPortStatEntry 33 }

LINKRESETTRANSMITTED

Object type	connUnitPortStatCountTxLinkResets
Description	The number of LRs transmitted ::= { connUnitPortStatEntry 34 }

LOSSOFSIGNALCOUNTER

Object type	connUnitPortStatCountLossofSignal
Description	The number of instances of signal loss detected at this port. This count is part of FC-PH's LESB. ::= { connUnitPortStatEntry 43 }

LOSSOFSYNCOUNTER

Object type	connUnitPortStatCountLossofSynchronization
Description	The number of instances of synchronization loss detected at this port. This count is part of FC-PH's LESB. ::= { connUnitPortStatEntry 44 }

MULTICASTFRAMESRECEIVED

Object type	connUnitPortStatCountRxMulticastObjects
Description	The number of multicast frames or packets received at this port ::= { connUnitPortStatEntry 29 }

MULTICASTFRAMESTRANSMITTED

Object type	connUnitPortStatCountTxMulticastObjects
Description	The number of multicast frames or packets transmitted through this port ::= { connUnitPortStatEntry 30 }

PBSYFRAMES

Object type	connUnitPortStatCountPBSYFrames
Description	The number of times that PBSY was returned to this port as a result of a frame that could not be delivered to the other end of the link. This occurs on SOFc1 frames (the frames that establish a connection) if the destination port is temporarily busy. This statistic is for Fibre Channel only. This is the sum of all classes. If you cannot keep the counters by class, keep the sum counters. ::= { connUnitPortStatEntry 11 }

PRIMITIVESEQPROTOCOLERRCOUNT

Object type	connUnitPortStatCountPrimitiveSequenceProtocolErrors
Description	The number of primitive sequence protocol errors detected at this port. This number is part of FC-PH's LESB. ::= { connUnitPortStatEntry 42 }

PRJTFRAMES

Object type	connUnitPortStatCountPRJTFrames
Description	The number of times that FRJT was returned to this port as a result of a frame being rejected at the destination N_Port. This is the total for all classes. ::= { connUnitPortStatEntry 13 }

RXCLASS1FRAMES

Object type	connUnitPortStatCountClass1RxFrames
Description	The number of Class 1 frames received at this port ::= { connUnitPortStatEntry 14 }

RXCLASS2FRAMES

Object type	connUnitPortStatCountClass2RxFrames
Description	The number of Class 2 frames received at this port ::= { connUnitPortStatEntry 20 }

RXCLASS3FRAMES

Object type	connUnitPortStatCountClass3RxFrames
Description	The number of Class 3 frames received at this port ::= { connUnitPortStatEntry 26 }

RXOFFLINESEQUENCES

Object type	connUnitPortStatCountRxOfflineSequences
Description	The number of Offline Primitive OLSs received at this port ::= { connUnitPortStatEntry 36 }

RXTRUNCFRAMES

Object type	connUnitPortStatCountFramesTruncated
Description	The number of frames received at this port where the frame length was less than the minimum indicated by the frame header, which is normally 24 bytes, but can be more if the DFCTL field indicates an optional header should have been present. ::= { connUnitPortStatEntry 47 }

TXOFFLINESEQUENCES

Object type	connUnitPortStatCountTxOfflineSequences
Description	The number of Offline Primitive OLSs transmitted by this port ::= { connUnitPortStatEntry 37 }

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 VCM. 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 you to upgrade, replace, or move servers within your enclosures without changes being visible to the external LAN/SAN environments.

Before getting started, perform the following tasks:

- Verify that the HP Onboard Administrator is running the latest firmware (must be v3.21 or later).
- Note the following information from the Default Network Settings label attached to the primary module:
  - DNS name
  - User name
  - Password
- Connect any Ethernet module stacking cables.

IMPORTANT: After a CLI command has completed, it can take up to 90 seconds before configuration changes are stored in persistent memory. Disruptive actions such as power 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 12):

- SSH

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

- LDAP Authentication

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

- RADIUS Authentication

```
>ssh 192.168.0.120
```

```
login as: <RADIUS user>
password: <password>
```

- TACACS+ Authentication

```
>ssh 192.168.0.120
login as: <TACACS+ user>
password: <password>
```

- Mechanism-based Authentication

```
>ssh 192.168.0.120
login as: <auth-mechanism>:<username>
password: <password>
```

Valid values for auth-mechanism are local, ldap, radius, and tacacs.

For example:

```
>ssh 192.168.0.120
login as: tacacs:<TACACS+ user>
password: <password>
```

- Role-based Authentication

```
>ssh 192.168.0.120
login as: <role>:<username>
password: <password>
```

Valid values for role are domain, network, server, and storage.

For example:

```
>ssh 192.168.0.120
login as: network:<username>
password: <password>
```

In role-based authentication, the role authentication order configured for the specified "role" will be used.

Domain setup

After logging in to the CLI (on page 125), perform the following tasks to set up the domain:

1. Import the enclosure ("Importing an enclosure" on page 126).
2. Name the domain ("Setting the domain name" on page 127).
3. Set up local user accounts and privileges ("Configuring local users" on page 127).
4. Set up authentication support for users:
   - LDAP authentication ("Configuring LDAP authentication support for users" on page 128)
   - RADIUS authentication ("Configuring RADIUS authentication support for users" on page 128)
   - TACACS+ authentication ("Configuring TACACS+ authentication support for users" on page 129)
5. Set up role-based authentication ("Configuring role-based authentication settings" on page 129).

Importing an enclosure

To import an enclosure, use the `import enclosure` command.

To enter OA credentials during import:

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

To be prompted for a masked password:

```
>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 31 characters without spaces or special characters.

Configuring local users

To add a new user:

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

To modify an existing user:

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

To remove an existing user:

```
>remove user bob
```

To remove all local users except for the Administrator account:

```
>remove user *
```

To display local user information:

- Summary of all users

  ```
  >show user
  ```

- Details for all users

  ```
  >show user *
  ```

- Details for a single user

  ```
  >show user steve
  ```

Up to 32 local user accounts can be created.

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

- Domain
  - Define local user accounts, set passwords, define roles
  - Configure role-based user authentication
  - 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

- Network
  - 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
  - Create, delete, and edit network access groups
  - 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 and UUIDs 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.

Configuring LDAP authentication support for users

To set LDAP properties:

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

To add LDAP directory groups:

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

To remove LDAP directory groups:

```
>remove ldap-group MyGroup
```

To enable or disable local users:

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

To display LDAP settings and directory groups:

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

Configuring RADIUS authentication support for users

To set RADIUS properties:

```
>set radius serveraddress=192.168.0.110 enabled=true serverkey=xyz1234
```

To add RADIUS groups:

```
>add radius-group MyNewGroup Description="Test Group"
Privileges=domain,server
```

To remove RADIUS groups:

```
>remove radius-group MyGroup
```

To display RADIUS settings and groups:

```
>show radius
>show radius-group
```

IMPORTANT: The RADIUS or TACACS+ server must be set up on a host machine on the management network and configured with users and VC attributes. For more information, see the *HP Virtual Connect for c-Class BladeSystem User Guide* on the Installing tab of the HP BladeSystem Technical Resources website (http://www.hp.com/go/bladesystem/documentation).

Configuring TACACS+ authentication support for users

To set TACACS+ properties:

```
>set tacacs serveraddress=192.168.0.110 enabled=true serverkey=xyz1234
```

To display TACACS+ settings:

```
>show tacacs
```

IMPORTANT: The RADIUS or TACACS+ server must be set up on a host machine on the management network and configured with users and VC attributes. For more information, see the *HP Virtual Connect for c-Class BladeSystem User Guide* on the Installing tab of the HP BladeSystem Technical Resources website (http://www.hp.com/go/bladesystem/documentation).

Configuring role-based authentication settings

To set the authentication order:

```
>set role domain Order=ldap,radius,tacacs
```

To display the authentication order:

```
>show role domain
```

Network setup

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

1. Identify the MAC addresses to be used on the server blades deployed within this Virtual Connect domain.
2. Set up 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

To configure MAC address ranges, use the `set domain` command.

To use VC-defined MAC addresses:

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

To use factory-default MAC addresses:

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

To 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 can assign MAC addresses that 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 assigns two MAC addresses to each VC-Enet connection in the server profile, a primary address for the Ethernet NIC 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.
- When FlexFabric adapters are in use, Virtual Connect assigns a MAC address to each FCoE connection in the server profile.
- When iSCSI connections are used, Virtual Connect assigns a MAC address to each iSCSI connection in the profile.

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 VCM and do not conflict with server factory default MAC addresses.

When using the HP-defined MAC address ranges, be sure 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 are not the 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.

  1024 unique addresses might not be enough for a large configuration (multiple enclosures with many Flex-10 NICs). If you plan a domain of this type, determine the number of MAC addresses you are likely to use, and then select an option that provides the domain with sufficient MAC addresses.

- 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 Insight Control Server Deployment for RedHat Linux installation and also plan to use User- or HP-defined MAC addresses, you must import the enclosure and assign profiles before running Insight Control Server Deployment.

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 a network access group

Before VC 3.30, any server profile could be assigned any set of networks. If policy dictated that some networks should not be accessed by a system that accessed other networks (for example, the Intranet and the Extranet) there was no way to enforce that policy automatically.

With VC 3.30 and later, network access groups are defined by the network administrator and associated with a set of networks that can be shared by a single server. Each server profile is associated with one network access group. A network cannot be assigned to the server profile unless it is a member of the network access group associated with that server profile. A network access group can contain multiple networks.

Up to 128 network access groups are supported in the domain. Ethernet networks and server profiles that are not assigned to a specific network access group are added to the domain Default network access group automatically. The Default network access group is predefined by VCM and cannot be removed or renamed.

If you are updating to VC 3.30, all current networks are added to the Default network access group and all server profiles are set to use the Default network access group. Network communication within the Default network access group behaves similarly to earlier versions of VC firmware, because all profiles can reach all networks.

If you create a new network access group, NetGroup1, and move existing networks from the Default network access group to NetGroup1, then a profile that uses NetGroup1 cannot use networks included in the Default network access group. Similarly, if you create a new network and assign it to NetGroup1 but not to the Default network access group, then a profile that uses the Default network access group cannot use the new network.

To create a network access group, use the `add network-access-group` command:

```
>add network-access-group MyGroupName
```

The network access group name must be unique within the data center, and can be up to 64 characters without spaces or special characters except for ".", "-", and "_".

Modifying network access groups

To modify network access groups, use the `set network-access-group` command:

```
>set network-access-group NetGroup1 Name=NewNetGroupName
```

- To add additional network members to the network access group, use the `add nag-network` command:
  ```
  >add nag-network nag=NetGroup1 network=Net3,Net4,Net5
  ```
- To remove specified network members from the network access group, use the `remove nag-network` command:
  ```
  >remove nag-network nag=NetworkGroup1 network=Net4,Net5
  ```

Displaying network access groups

To display network access groups, use the `show network-access-group` command:

- Summary for all network access groups
  ```
  >show network-access-group
  ```
- Details for all network access groups
  ```
  >show network-access-group *
  ```
- Details for a network access group
  ```
  >show network-access-group MyGroupName
  ```

To display the members of network access groups, use the `show nag-network` command:

```
>show nag-network *
```

Creating an Ethernet network

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

```
>add network MyNetworkName
```

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

Modifying Ethernet network properties

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

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

Displaying Ethernet networks

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

- Summary of all networks
  ```
  >show network
  ```
- Details for all networks
  ```
  >show network *
  ```
- Details for a single network
  ```
  >show network MyNetwork
  ```

Adding Ethernet networks to a network access group

To add existing network access groups to an existing network, use the `add nag-network` command:

```
>add nag-network Nag=DatabaseNetGroup Network=Net1,Net2
```

The networks become members of the specified network access group in addition to all the previously configured network access groups.

To modify the network access groups of an existing network, use the `set network` command:

```
>set network Net1 nags=NetGroup1,NetGroup2
```

The specified network now belongs to the specified network access groups and is no longer the member of previously configured network access groups.

Creating an Ethernet network that uses network access groups

To create a network that is assigned to network access groups DatabaseNetGroup and AccessNetGroup, use the `add network` command:

```
>add network Network1 nags=DatabaseNetGroup,AccessNetGroup
```

Adding uplink ports to an Ethernet 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 set

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

```
>add uplinkset MyUplinkSetName
```

A shared uplink set identifies VC-Enet module uplinks that carry multiple networks over the same cable or set of cables. 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 VCM must be configured to use the same VLAN tag identifier (a number between 1 and 4094) for each network.

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.

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 outgoing Ethernet packets are VLAN-tagged.

Displaying shared uplink sets

To display shared uplink sets, use the `show uplinkset` command:

- Summary for all shared uplink sets
  ```
  >show uplinkset
  ```
- Details for all shared uplink sets
  ```
  >show uplinkset *
  ```
- Details for a single shared uplink set
  ```
  >show uplinkset MyUplinkSetName
  ```

Adding uplink ports to a shared uplink set

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

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

Creating a network that uses a shared uplink set

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

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

Creating multiple networks that use a shared uplink set

To create multiple networks that use a shared uplink set, use the `add network-range` command:

```
>add network-range UplinkSet=SUS1 VLANIds=
```

Server VLAN Tagging Support

Each server port can be connected to multiple virtual networks, each using a unique server VLAN ID for virtual network mapping.

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. 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:

```
>set enet-vlan SharedServerVLanID=true
```

Setting the value to "false" enables you to select any VC Ethernet network for the server Ethernet connections, and VLAN ID mappings can be modified to ensure uniqueness:

```
>set enet-vlan SharedServerVLanID=false
```

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
```

VLAN Capacity

Virtual Connect imposes certain limits on the number of networks (VLANs) in the domain and the server connections carrying multiple VLANs. In a VC domain that does not contain legacy (1/10Gb) VC Ethernet modules, these restrictions can be relaxed to provide support for more VLANs and enhance the flexibility of mapping VLANs to server connections. When VCM detects that no legacy modules are present in the domain, it enables the selection of a new domain mode that expands the VLAN capacity. The increase in the number of VLANs per domain, in addition to the flexibility of allocating VLANs among the server connections for a physical port, provides you with more options when configuring a Virtual Connect environment.

CAUTION: If VCEM is managing the domain, be sure that the VCDG containing the domain is running at a firmware mode of 3.30 or higher before applying VLAN capacity changes. Failure to do so requires removal of the domain from the VCEM VCDG.

Legacy VLAN capacity

This mode has the same limits as previous releases of Virtual Connect. There is a limit of 320 VLANs per Ethernet module and 128 VLANs per shared uplink set. Every VLAN on every uplink counts towards the 320 VLAN limit. If a shared uplink set is comprised of multiple uplinks, each VLAN on that shared uplink set is counted multiple times. In addition, each server connection is limited to 28 VLANs. If less than 28 VLANs are used on a server connection, the remaining capacity is not made available to other server connections on the same physical server port. All VC Ethernet modules are supported.

Expanded VLAN capacity

This mode allows up to 1000 VLANs per domain. The number of VLANs per shared uplink set is restricted to 1000. In addition, up to 162 VLANs are allowed per physical server port, with no restriction on how those VLANs are distributed among the server connections mapped to the same physical server port. There is also a limit of 162 VLANs per server connection. However, care must be taken not to exceed the limit per physical server port. For example, if you configure 150 VLAN mappings for a server connection (FlexNIC-a) of a Flex-10 physical server port, then you can only map 12 VLANs to the remaining three server connections (FlexNIC-b, FlexNIC-c, and FlexNIC-d) of the same physical server port. If you exceed the 162 VLAN limit, the physical server port is disabled and the four server connections are marked as Failed.

CAUTION: After Expanded VLAN Capacity mode is configured, you must delete the VC domain to return to Legacy VLAN Capacity mode.

IMPORTANT: Expanded VLAN Capacity mode is not supported on the following VC Ethernet modules:

- HP 1/10Gb VC-Enet Module
- HP 1/10Gb-F VC-Enet Module

If these modules are inserted into an enclosure that is in Expanded VLAN Capacity mode, they are marked as incompatible.

The default value is "Legacy". Set the `VlanResourceMode` to "Expanded" to use expanded VLAN capacity:

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

Fibre Channel setup

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

1. Identify WWNs to be used on the server blades deployed within this Virtual Connect domain.
2. Create FC SAN fabrics ("Creating FC fabrics" on page 136).

Configuring WWN address ranges

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 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 FC HBA ports, Virtual Connect assigns 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.

Virtual Connect assigns or migrates WWNs for server FC ports connected to HP Virtual Connect modules. Virtual Connect also assigns WWNs to FC ports that are not connected to an I/O module because Virtual Connect modules can be added later. Server FC ports connected to non-Virtual Connect modules retain the server factory default WWNs.

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 do 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.

To configure WWN address ranges, use the `set domain` command:

- VC-defined

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

- Factory default

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

Creating FC fabrics

To create an FC SAN fabric and add it to the domain, use the `add fabric` command:

```
>add fabric MyFabric2 Bay=3 Ports=1 Speed=2Gb
```

Displaying FC fabrics

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

```
>show fabric
```

Serial number settings

The serial number settings feature enables you to add a serial number and UUID to server profiles. The UUIDs that Virtual Connect assigns are randomly generated. A UUID pool is not required.

By configuring VCM to assign serial numbers, a profile can present a single serial number regardless of the physical server. With these configuration values added to server profiles, software that is licensed to a particular server, based on one or both of these values, can be migrated to new server hardware without

re-licensing the software for the new server hardware. This feature prevents you from having to reinstall serial number sensitive software after a system recovery.

If you need to access the physical serial number of a server blade, the Onboard Administrator displays both the physical and assigned serial numbers.

After server profile creation, the following guidelines apply:

- Serial numbers can be changed from factory default to VC-assigned.
- Factory default serial numbers cannot be changed.
- User-defined serial number ranges can be expanded.
- User-defined serial number ranges cannot be reduced.

> △ **CAUTION:** The use of Serial Number Settings might prevent the proper operation of software designed to track servers by serial number or UUID. Do not enable this feature until you consider and understand the impact to the entire software environment in which the servers operate. This impact includes, but is not limited to, warranty service, asset tracking, server deployment, and software licensing.

Configuring serial number ranges

To configure serial number ranges, use the `set serverid` command:

- 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

The I/O connection profile, or server profile, provides a link between the server and the networks and fabrics defined in VC. The server profile can include MAC and WWN addresses, as well as boot parameters for the various connection protocols supported by VC. After being defined, the server profile can be assigned to any server blade within the Virtual Connect domain. VCM supports up to 256 profiles within the domain.

A Virtual Connect server profile consists of connections that group attributes related to server connectivity for the various protocols supported by Virtual Connect modules. These protocols are Ethernet, iSCSI, Fibre Channel over Ethernet (FCoE), and Fibre Channel.

- For Ethernet connections, VC provides the ability to assign VC-assigned MAC addresses and configure PXE boot settings as well as allocate bandwidth on Flex-10 connections.
- For iSCSI connections, VC provides the ability to assign VC-assigned MAC addresses and configure iSCSI boot settings as well as allocate bandwidth. This protocol is only available on Flex-10 server ports that support iSCSI.
- For FCoE connections, VC provides the ability to assign VC-assigned WWN and MAC addresses and configure Fibre Channel boot settings and bandwidth. This protocol is only available on FlexFabric server connections.
- For FC connections, VC provides the ability to assign VC-assigned WWN addresses and configure Fibre Channel boot settings.

IMPORTANT: The term server blade also applies to HP Integrity multi-blade servers. For more information on multi-blade servers, see the *HP Virtual Connect Manager for c-Class BladeSystem User Guide*.

When a server profile is assigned to a server blade, VCM configures the connections with the appropriate MAC/WWN addresses and boot settings. USE BIOS is an option for all connection boot settings that preserves the options set in the RBSU or through other configuration utilities. Virtual Connect Manager automatically connects the server blade Ethernet, iSCSI, FCoE, 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.

VCM 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 the host operating system software as the hardware addresses. To use administered MAC/WWN addresses, select a range of HP pre-defined or user-specified MAC addresses.

Review the following list of guidelines before creating and deploying server profiles:

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 (on page 143)."

- 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 assigned serial numbers or factory default serial numbers.
  - Select whether to use movable, administered MAC addresses and WWNs, or the local server blade factory default MAC addresses and WWNs.
- After an enclosure is imported into a Virtual Connect domain, server blades are 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 or FlexFabric modules, there are special considerations for server power.
- When assigning a VC-assigned serial number, the server must be powered off.
- FC SAN connections appear in server profile screens only when an HP Virtual Connect Fibre Channel module is 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 when editing existing profiles.
- FCoE connections appear in server profile screens only when an HP VC Flex Fabric 10Gb/24-port Module is in the enclosure managed by Virtual Connect. FCoE SAN connections are added in pairs. If an HP VC Flex Fabric 10Gb/24-port Module is added to a Virtual Connect domain with existing profiles, you can add FCoE connections.
- iSCSI connections are not added to server profiles by default. You must add one or more iSCSI connections. The GUI enables the creation of iSCSI connections only if at least one Flex-10 or FlexFabric module exists in the domain. The CLI can be used to pre-provision this feature. iSCSI and FCoE connections cannot share the same physical Flex-10 port since they use the same physical function.

- 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 restores the settings defined by the server profile after the server blade completes the next boot cycle.
- After Virtual Connect assigns a server profile to a server, RBSU cannot modify the protocol configuration (iSCSI/FCoE) for any NIC, including the NC551m, even if the NIC is not connected to a Virtual Connect module. Any protocol configuration changes must be made before the server profile is assigned to the server.
- 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.
- If the VC domain is configured for double-dense server mode and a profile is assigned to an empty server bay, a hot-plug installation of a single-dense server into that server bay results in the profile not being activated. To recover the profile, unassign the profile, and then reassign it.
- During a profile assignment, if the port number of an existing fabric has been changed to another physical port, the fabric and the domain go into a failed state until the reconfiguration is complete. This also might result in SNMP traps being sent to report the interim failed state.

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, and 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 boot and gain access to the network and fabric when the server and interconnect modules are ready.

If a server blade is installed in a device bay already assigned a server profile, Virtual Connect Manager automatically updates the configuration of that server blade before it can power on 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.

Creating server profiles

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

```
>add profile MyNewProfile
```

To copy the configuration from one profile to another profile, use the following command:

```
>copy ExistingProfile MyNewProfile
```

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 enable deployment at a later date.

Adding Ethernet 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
>add server-port-map-range MyProfile:1 VLanIds=151-170,215
```

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 iSCSI connections to a profile

To add a new iSCSI connection to an existing server profile, use the `add iscsi-connection` command:

```
>add iscsi-connection MyProfile network=MyNetwork speedType=custom
speed=2000
```

To configure the boot parameters for the iSCSI connection, use the `set iscsi-boot-param command` as follows:

```
>set iscsi-boot-param MyProfile1:1 BootOrder=Primary Lun=100
InitiatorName="iqn.2009-09.com.someorg.iSCSI-Initiator"
InitiatorIp=192.128.3.1 Mask=255.255.0.0
TargetName="iqn.2009-09.com.someorg.iSCSI-Target" TargetIp=192.128.3.2
TargetPort=40000 Authentication=CHAP Username=SomeUserName
Secret=SomePassword123
```

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
```

For more information, see "General requirements for adding FC or FCoE connections (on page 144)."

Adding FCoE connections to a profile

To add a new FCoE connection to an existing server profile, use the `add fcoe-connection` command:

```
>add fcoe-connection MyNewProfile Fabric=SAN_1 SpeedType=Custom
CustomSpeed=5000
```

To configure the boot parameters for the FCoE connection, use the `set fcoe-connection` command:

```
>set fcoe-connection MyNewProfile:1 BootPriority=Primary
BootPort=50:06:0B:00:00:C2:62:00 BootLun=5
```

For more information, see "General requirements for adding FC or FCoE connections (on page 144)."

Adding a network access group to a profile

To create a new profile and assign an existing network access group, use the `add profile` command:

```
>add profile MyNewProfile2 Nag=DatabaseNetGroup
```

To modify the network access group of an existing server profile, use the `set profile` command:

```
>set profile Profile1 Nag=NetGroup1
```

Assigning a server profile to a device bay

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

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

When defining server profiles in a multi-enclosure configuration, profiles can be assigned to server bays in any of the enclosures that have been added and imported into the domain.

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. Be sure that the profile contains enough Ethernet and Fibre Channel connection entries for all of the ports on all of the blades in the multi-blade server.

Configuring IGMP settings

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

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

The IGMP Snooping feature enables VC-Enet modules to monitor (snoop) the IGMP IP multicast membership activities and configure hardware Layer 2 switching behavior of multicast traffic to optimize network resource usage. IGMP v1, v2, and v3 snooping are supported.

The IGMP Snooping idle timeout interval is set to 260 seconds by default. This value is 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.

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, external Ethernet switches can take several minutes 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 (HP recommends 5 seconds) and completes in about 1 minute.

Virtual Connect only transmits MAC Cache update frames on VLANs that have been configured in the VC domain. The update frames are VLAN tagged appropriately for networks defined on shared uplink sets. For dedicated networks, only untagged update frames are generated, regardless of whether or not VLAN Tunneling is enabled. In a VLAN tunnel, all customer VLAN tags pass through Virtual Connect transparently. Virtual Connect does not examine nor record VLAN tag information in tunneled networks; therefore, it cannot generate tagged update frames.

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.
Always enable the "spanning tree portfast" feature to allow the switch port to bypass the "listening" and "learning" stages of spanning tree and quickly transition to the "forwarding" stage, allowing edge devices to immediately begin communication on the network.

Configuring network loop protection settings

To enable network loop protection, use the `set loop-protect` command:

```
>set loop-protect Enabled=true
```

To reset network loop protection, use the `reset loop-protect` command:

```
>reset loop-protect
```

To avoid network loops, Virtual Connect first verifies that only one active uplink exists per network from the Virtual Connect domain to the external Ethernet switching environment. Second, Virtual Connect makes sure that no network loops are created by the stacking links between Virtual Connect modules.

- One active link—A VC uplink set can include multiple uplink ports. To prevent a loop with broadcast traffic coming in one uplink and going out another, only one uplink or uplink LAG is active at a time. The uplink or LAG with the greatest bandwidth should be selected as the active uplink. If the active uplink loses the link, then the next best uplink is made active.
- No loops through stacking links—If multiple VC-Enet modules are used, they are interconnected using stacking links, which might appear as an opportunity for loops within the VC environment. For each individual network in the Virtual Connect environment, VC blocks certain stacking links to ensure that each network has a loop-free topology.

Enhanced network loop protection detects loops on downlink ports, which can be a Flex-10 logical port or physical port. The feature applies to Flex-10 logical function if the Flex-10 port is operating under the control of DCC protocol. If DCC is not available, the feature applies to a physical downlink port.

Enhanced network loop protection uses two methods to detect loops:

- It periodically injects a special probe frame into the VC domain and monitors downlink ports for the looped back probe frame. If this special probe frame is detected on downlink ports, the port is considered to cause the loop condition.
- It monitors and intercepts common loop detection frames used in other switches. In network environments where the upstream switches send loop detection frames, the VC Enet modules must ensure that any downlink loops do not cause these frames to be sent back to the uplink ports. Even though VC probe frames ensure loops are detected, there is a small time window depending on the probe frame transmission interval in which the loop detection frames from the external switch might loop through down link ports and reach uplink ports. By intercepting the external loop detection frames on downlinks, the possibility of triggering loop protection on the upstream switch is eliminated. When network loop protection is enabled, VC-Enet modules intercept the following types of loop detection frames:
  - PVST+ BPDUs
  - Procurve Loop Protect frames

When the network loop protection feature is enabled, any probe frame or other supported loop detection frame received on a downlink port is considered to be causing the network loop, and the port is disabled immediately until an administrative action is taken. The administrative action involves resolving the loop condition and clearing the loop protection error condition. The "loop detected" status on a port can be cleared by one of the following administrative actions:

- Restart loop detection by issuing "reset" loop protection from the CLI or GUI
- Unassign all networks from the port in "loop detected" state

The SNMP agent supports trap generation when a loop condition is detected or cleared.

Virtual Connect provides the ability to enable or disable network loop protection. The feature is enabled by default and applies to all VC-Enet modules in the domain. Network loops are detected and server ports can be disabled even prior to any enclosure being imported.

A loop-protect reset command resets and restarts loop detection for all server ports in a "loop-detected" error condition.

Server blade power on and power off guidelines

Certain server profile changes require the server blade in the device bay to be powered off before the change can be made. HP recommends that administrators power off servers with the server console before attempting such operations within the Virtual Connect Manager.

If any changes are made to a server profile that require modifications to the server, the server blade must be powered off. Network or fabric changes do not require the server blade to be powered off. Server side settings include the following:

- Assigning a VC- or user-defined MAC address
- Changing the PXE setting
- Assigning a VC-defined WWN
- Changing the Fibre Channel boot parameters
- Changing iSCSI boot parameters
- Adding or deleting a connection of any kind

If any of the listed settings are changing, the server must be powered off before the profile action can occur. If the server blade is not powered off, a message appears and no changes are made. In this case, power off the server blade and repeat the action.

When server side settings are changing, the following operations require that server blades be powered off:

- Assigning a profile to a server blade already installed in a device bay
- Deleting a profile, moving a profile to a different device bay, or unassigning a profile from the existing bay
- Making modifications to a profile that affect settings on the server blade; for example, PXE enable/disable, changing the number of connections, or changing Fibre Channel boot parameters
- Assigning a VC-assigned serial number

The following operations do not require the server blade to be powered off:

- Changing the network connected to an already defined Ethernet port
- Changing the Fabric connected to a Fibre Channel port
- Changing the speed of a Fibre Channel port
- Assigning or unassigning server profiles, if server factory defaults are used for MAC addresses and WWNs, BIOS Fibre Channel boot settings are used, and PXE is not being enabled or disabled (USE BIOS for all network connections)

  Exceptions for Flex-10 connection changes are specified in the following sections.

Flex-10 connection changes that require power off

Always power off server blades with Flex-10 connections in the following instances:

- Adding a connection that is mapped to Flex-10

- Removing a connection that is mapped to Flex-10
- Assigning a profile to a server that maps Flex-10 connections
- Unassigning a profile with Flex-10 connections

Flex-10 connection changes that do not require power off

With Virtual Connect Manager v2.10 and higher, it is not necessary to power off a server blade with Flex-10 connections in the following instances:

- Changing a connection's network:
  - From a single network to another single network
  - From a single network to multiple networks
  - From multiple networks to a single network
- Modifying the networks or VLAN IDs in a connection with multiple networks

With Virtual Connect Manager v2.30 and higher, it is not necessary to power off a server blade with Flex-10 connections in the following instances:

- Changing a connection's network:
  - From "unassigned" to a single network
  - From a single network to "unassigned"
  - From "unassigned" to multiple networks
  - From multiple networks to "unassigned"
- Changing the requested bandwidth

FCoE connection changes that require power off

- Adding an FCoE connection to an assigned server profile
- Removing an FCoE connection from an assigned server profile
- Assigning a profile containing FCoE connections to a server
- Changing FCoE boot parameters

Restart after OA credential recovery

The state, "profile recovered," is applied to servers that are powered on when VC Manager restarts after an OA credential recovery. When VC Manager detects a restart after a credential recovery, it rewrites the profile parameters for any server that is powered on, connects the server to the appropriate Ethernet networks and FC fabrics, and then puts the server and profile in the "profile recovered" state. The server and profile remain in the "profile recovered" state until the server is powered down or removed from the enclosure. This feature eliminates the power cycle requirement for a server to recover.

General requirements for adding FC or FCoE connections

Adding FC and FCoE connections is generally allowed during profile add and edit operations. It is not allowed in some specific cases. Observe the following general requirements:

- When a profile is added, the FC/FCoE connections initially displayed are based on the FC/FCoE module configuration in the domain, respectively. A pair of horizontally adjacent FC/FCoE-capable modules has two connections.
- Connections can only be added or removed from the bottom. You can only add or delete connections at the end of the list.

- You can remove connections at any time (one at a time, from the bottom).
- If the existing profile connections do not match the current FC/FCoE module configurations, the add operation is not allowed.
- The current maximum number of FC/FCoE connections is four per I/O bay.

The following table lists several scenarios that describe how adding FC/FCoE connections affects an existing profile. The scenarios are true for FC module configurations and FC modules, as well as FCoE module configurations and FCoE-capable modules.

Scenario	Description	Existing profile connections	Current FC module configurations	Adding profile connections
1	Start with modules in Bays 3 and 4, create a profile, then edit the profile and add connections.	*Port* *Connected to* 1 Bay 3 2 Bay 4	— — Bay 3 Bay 4 — — — —	*Port* *Connected to* 1 Bay 3 2 Bay 4 3 Bay 3 4 Bay 4 Add connection, 2 times
2	Start with modules in Bays 3–6, create a profile, then edit the profile and add connections.	*Port* *Connected to* 1 Bay 3 2 Bay 4 3 Bay 5 4 Bay 6	— — Bay 3 Bay 4 Bay 5 Bay 6 — —	*Port* *Connected to* 1 Bay 3 2 Bay 4 3 Bay 5 4 Bay 6 5 Bay 3 6 Bay 4 7 Bay 5 8 Bay 6 Add connection, 4 times
3	Start with modules in Bays 3 and 4, create a profile, hotplug modules into Bays 5 and 6, then edit the profile and add connections.	*Port* *Connected to* 1 Bay 3 2 Bay 4	— — Bay 3 Bay 4 Bay 5 Bay 6 — —	*Port* *Connected to* 1 Bay 3 2 Bay 4 3 Bay 5 4 Bay 6 Add connection, 2 times
4	Start with modules in Bays 3 and 4, create a profile (add 2 connections), hotplug modules into Bays 5 and 6, then edit the profile.	*Port* *Connected to* 1 Bay 3 2 Bay 4 3 Bay 3 4 Bay 4	— — Bay 3 Bay 4 Bay 5 Bay 6 — —	Add connection is disallowed because the current FC module configurations do not match the existing connections in the profile. This profile is not useful after the hotplug. To resolve this issue, delete connections 3 and 4, save the profile, and then scenario 3 applies.
5	Start with modules in Bays 3–6, create a profile, hotplug modules into Bays 7 and 8, then edit the profile and add connections.	*Port* *Connected to* 1 Bay 3 2 Bay 4 3 Bay 5 4 Bay 6	— — Bay 3 Bay 4 Bay 5 Bay 6 Bay 7 Bay 8	*Port* *Connected to* 1 Bay 3 2 Bay 4 3 Bay 5 4 Bay 6 5 Bay 7 6 Bay 8 Add connection, 2 times

6	Start with modules in Bays 3–6, create a profile (add 4 connections), hotplug modules into Bays 7 and 8, then edit the profile.	*Port* *Connected to* 1 Bay 3 2 Bay 4 3 Bay 5 4 Bay 6 5 Bay 3 6 Bay 4 7 Bay 5 8 Bay 6	— — Bay 3 Bay 4 Bay 5 Bay 6 Bay 7 Bay 8	Add connection is disallowed because the current FC module configurations do not match the existing connections in the profile. This profile is not useful after the hotplug. To resolve this issue, delete connections 5–8, save the profile, and then scenario 5 applies.
7	Start with modules in Bays 5 and 6, create a profile, hotplug modules into Bays 3 and 4, then edit the profile.	*Port* *Connected to* 1 Bay 5 2 Bay 6	— — Bay 3 Bay 4 Bay 5 Bay 6 — —	Add connection is disallowed because the current FC module configurations do not match the existing connections in the profile.
8	Start with modules in Bays 5–8, create a profile, hotplug modules into Bays 3 and 4, then edit the profile.	*Port* *Connected to* 1 Bay 5 2 Bay 6 4 Bay 7 5 Bay 8	— — Bay 3 Bay 4 Bay 5 Bay 6 Bay 7 Bay 8	Add connection is disallowed because the current FC module configurations do not match the existing connections in the profile.
9	Start with FCoE-capable modules in Bays 1 and 2, then create a profile and add connections.	*Port* *Connected to* 1 Bay 1 2 Bay 2	Bay 1 Bay 2 — — — — — —	*Port* *Connected to* 1 Bay 1 2 Bay 2 3 Bay 1 4 Bay 2 5 Bay 1 6 Bay 2 7 Bay 1 8 Bay 2 Add connection, 6 times

10	Start with 8 FCoE-capable modules, then create a profile and add connections.	*Port*	*Connected to*	Bay 1	Bay 2	*Port*	*Connected to*
		1	Bay 1	Bay 3	Bay 4	1	Bay 1
		2	Bay 2	Bay 5	Bay 6	2	Bay 2
		3	Bay 3	Bay 7	Bay 8	3	Bay 3
		4	Bay 4			4	Bay 4
		5	Bay 5			5	Bay 5
		6	Bay 6			6	Bay 6
		7	Bay 7			7	Bay 7
		8	Bay 8			8	Bay 8
						9	Bay 1
						10	Bay 2
						11	Bay 3
						12	Bay 4
						13	Bay 5
						14	Bay 6
						15	Bay 7
						16	Bay 8
						17	Bay 1
						18	Bay 2
						19	Bay 3*
						20	Bay 4*
						21	Bay 5*
						22	Bay 6*
						23	Bay 7*
						24	Bay 8*
						25	Bay 1
						26	Bay 2
						*Not mapped	
						Add connection, 18 times	

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 more 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`

Operation	Examples
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 backup 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`

Port status conditions

If a port status is unlinked and no connectivity exists, one of the following causes appears:

- **Not Linked/E-Key**—The port is not linked due to an electronic keying error. For example, a mismatch in the type of technology exists between the server and module ports.
- **Not Logged In**—The port is not logged in to the remote device.
- **Incompatible**—The port is populated with an SFP module that does not match the usage assigned to the port, such as a Fibre Channel SFP connected to a port designated for Ethernet network traffic. A port that is not assigned to a specific function is assumed to be designated for Ethernet network traffic.

  An FCoE-capable port that has an SFP-FC module connected that is not yet assigned to a fabric or network is designated for a network, and the status is "Incompatible." When a fabric is created on that port, the status changes to "Linked."
- **Unsupported**—The port is populated with an SFP module that is not supported. For example:
  - An unsupported module is connected.
  - A 1Gb or 10Gb Ethernet module is connected to a port that does not support that particular speed.
  - An LRM module is connected to a port that is not LRM-capable.
  - An FC module is connected to a port that is not FC-capable.

- **Administratively Disabled**—The port has been disabled by an administrative action, such as setting the uplink port speed to 'disabled.'
- **Unpopulated**—The port does not have an SFP module connected.
- **Unrecognized**—The SFP module connected to the port cannot be identified.
- **Failed Validation**—The SFP module connected to the port failed HPID validation.
- **Smart Link**—The Smart Link feature is enabled.
- **Not Linked/Loop Protected**—VCM is intercepting BPDU packets on the server downlink ports and has disabled the server downlink port to prevent a loop condition.
- **Linked/Uncertified**—The port is linked to another port, but the connected SFP module is not certified by HP to be fully compatible. In this case, the SFP module might not work properly. Use certified modules to ensure server traffic.

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 backup Ethernet module, you can use this feature to manually change which Virtual Connect Ethernet module hosts the Virtual Connect Manager. You 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 backup Virtual Connect Ethernet module is available, the command line displays the following message:

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

You are 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 you attempt to log in to the backup module, you might receive the following error message:

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

The login should succeed after the Virtual Connect Manager restarts on the backup 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 backup Virtual Connect Ethernet module is not available, the command line displays the following message:

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

You are logged out of the session after approximately 1 minute. If you attempt to log in to the module again, you might receive the following error message:

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

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

Support and other resources

Before you contact HP

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

- Active Health System log

  Download and have available an Active Health System log for 3 days before the failure was detected. For more information, see the *HP iLO 4 User Guide* or *HP Intelligent Provisioning User Guide* on the HP website (http://www.hp.com/go/ilo/docs).

- Onboard Administrator SHOW ALL report (for HP BladeSystem products only)

  For more information on obtaining the Onboard Administrator SHOW ALL report, see the HP website (http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c02843807).

- 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 United States and worldwide contact information, see the Contact HP website (http://www.hp.com/go/assistance).

In the United States:

- To contact HP by phone, call 1-800-334-5144. For continuous quality improvement, calls may be recorded or monitored.
- If you have purchased a Care Pack (service upgrade), see the Support & Drivers website (http://www8.hp.com/us/en/support-drivers.html). If the problem cannot be resolved at the website, call 1-800-633-3600. For more information about Care Packs, see the HP website (http://pro-aq-sama.houston.hp.com/services/cache/10950-0-0-225-121.html).

Acronyms and abbreviations

BPDU

Bridge Protocol Data Unit

CHAP

Challenge Handshake Authentication Protocol

CHAPM

Mutual Challenge Handshake Authentication Protocol

CRC

cyclic redundant checks

DCBX

Datacenter Bridging Capability Exchange protocol

DCC

device control channel

DHCP

Dynamic Host Configuration Protocol

DNS

domain name system

EFI

extensible firmware interface

FC

Fibre Channel

FCoE

Fibre Channel over Ethernet

FCS

Frame Check Sequence

GMII

Gigabit media independent interface

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

LLC

Logical Link Control

LUN

logical unit number

MAC

Media Access Control

NPIV

N_Port ID Virtualization

OA

Onboard Administrator

PVST+

Per VLAN Spanning Tree (over standard 802.1q links)

PXE

preboot execution environment

RADIUS

Remote Authentication Dial-In User Service

RD

receive data

RMON

remote monitoring

SOAP

Simple Object Access Protocol

SSH

Secure Shell

SSL

Secure Sockets Layer

TACACS+

Terminal Access Controller Access Control System Plus

TFTP

Trivial File Transfer Protocol

UDP

User Datagram Protocol

UUID

universally unique identifier

VC

Virtual Connect

VCEM

Virtual Connect Enterprise Manager

VCM

Virtual Connect Manager

VCSU

Virtual Connect Support Utility

VLAN

virtual local-area network

WWN

World Wide Name

WWPN

worldwide port name

Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (mailto:docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

Index

L

M

N

O

P

R

S

T

U

V

W