Voltaire® 4036/2036 Grid Director

User Manual

4036/2036 Software Version: 2.0

April 2009
Doc P/N: DOC-00619
Rev: A01

Voltaire Document Part Number: DOC-00619

Business Headquarters
Voltaire Inc.
6 Fortune Drive, Suite 301
Billerica, MA
USA 01821
Tel: 978-439-5400
Fax: 978-439-5401

R&D Center
Voltaire Ltd.
13 Zarchin St
Raanana 43662
Israel
Tel: +972-74-7129000
Fax: +972-74-7129111

Overview

Voltaire's integrated family of switching hardware and network virtualization software delivers a high-performance, intelligent solution for deploying clusters and grids. Leveraging InfiniBand technology, Voltaire solutions offer improved application performance, resource utilization and data center scalability for its customers' high-performance computing needs. Voltaire switching solutions are available in a multitude of port counts to facilitate the deployment of powerful clusters ranging from a few to thousands of nodes.

The 4036 and the 2036 are part of the Grid Director family:

This Manual is divided as follows:

- Part 1: Getting Started and Voltaire Device Manager
- Part 2: CLI Reference Section
- Part 3: Appendix and Glossary

NOTE:

Terms and CLI examples are interchangeable between the 2036 and 4036 unless specified otherwise.

CAUTION:

Voltaire highly recommends against using root permissions for its switches. Use of root permission for the switches is at the user's own risk.

About this Manual

This preface describes the audience, organization and command syntax conventions of this *4036/2036 User Manual*. It also provides information on how to obtain related documentation and technical assistance.

Information about hardware installation of the respective Voltaire switches can be found in the *4036/2036 Installation Manual* [DOC-00467]

NOTE:

Refer to the latest Voltaire release notes for last minute updates and restrictions.

The Voltaire Technical Support Center (TSC) is at your service. You may access Warranty Service through our Web Request Form by using the following link: http://www.voltaire.com/support.html

Contact Us:

Please send your documentation-related comments and feedback or report mistakes to docs@Voltaire.com.

We are committed to constant and never-ending improvement. Your input will greatly help us in our endeavor.

Audience

This manual is primarily intended for system administrators who are familiar with the fundamentals of router-based internetworking and network storage devices, but who might not be familiar with the specifics of Voltaire products or the routing protocols supported by Voltaire products

It is assumed that readers are familiar with InfiniBand technology and terminology.

Related Documentation

- 4036/2036 Getting Started Guide - Voltaire QDR Solution (LIT-00037)
- Voltaire 4036/2036 Installation Manual [DOC-00467]
- Unified Fabric Manager (UFM) User Manual, Voltaire [DOC-00600]

Document Conventions

NOTE:

Text set off in this manner presents clarifying information, specific instructions, commentary, sidelights, or interesting points of information.

IMPORTANT:

Text set off in this manner indicates important information regarding a specific feature.

CAUTION:

Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

Contents

Figures

Tables

PART 1:

4036/2036 Device Manager

Chapter 1. Introduction

In This Chapter:

This chapter provides a brief introduction to InfiniBand technology and describes the Voltaire product family.

It includes information on the following topics:

1.1 About InfiniBand

InfiniBand technology is a high-performance channel-based interconnect architecture that provides increased scalability and reliability for servers and other Internet infrastructure equipment. InfiniBand architecture defines the entire stack, from the physical to the application layers APIs and fabric management.

InfiniBand has unique capabilities for direct data placement implemented by RDMA and for OS bypassing, discovery, fail-over, remote boot, I/O sharing, and other advanced features.

InfiniBand is the IT industry's solution for expanding data network centers to prepare for the next generation of communications. High Performance datacenters with high performance applications have created the need for increased processing power, larger stores of information and a greater, more reliable flow of data. As the present architecture struggled under the current load of information, it was painfully clear that a solution was needed in order to manage the increasing demands of the future. The giants of the IT industry (Compaq, Dell, IBM, Intel, HP, SUN and Microsoft followed by more than 230 companies) combined the best elements of two competing technological initiatives to create InfiniBand, an industry standard that has been adopted with confidence. Solving a great number of obstacles that data centers were facing (scalability, reliability, manageability), InfiniBand enabled the introduction of data clusters, an invaluable next step to data center construction.

In effect, InfiniBand is a fabric-based, switched network that allows devices such as servers, storage and I/O to communicate at very high speeds. Until the advent of InfiniBand, communication devices had to wait in line to send their information through one shared bus. The ten-year-old architecture had reached its limits and did not have enough bandwidth available to meet the rising demands of the information load.

InfiniBand architecture is based upon a very different concept. Offering high-speed interprocessor communication and memory sharing, it enables you to build server clusters with performance comparable to that of large servers at a fraction of the price. Instead of one bus through which every device communicates, InfiniBand architecture offers a network fabric that incorporates numerous switches and I/O Gateway modules, allowing devices to communicate simultaneously. Speed is no longer restricted by the shortcomings of the infrastructure. InfiniBand operates at 2.5Gbps (1X), 10Gbps (SDR), 20Gbps (DDR), and 40Gbps (QDR).

InfiniBand architecture is modular, highly scalable (it allows for virtually unlimited network expansion) and reduces the workload of the operating system kernel and the CPU, freeing their power to run applications. Offering advanced fault isolation controls, nonexistent in previous protocols, InfiniBand provides a high level of fault tolerance. Moreover, most importantly, because the InfiniBand system is modular, processing power based on commodity servers can be added as needed.

InfiniBand System Elements

The following are the InfiniBand system elements:

- **HCA** (Host Channel Adapter), an adapter or silicon chip residing on the host motherboard providing the host side functionality and advanced reliable message passing capabilities.
- **InfiniBand Protocol Stack,** the software required by the operating system on the server to recognize the HCA. Includes additional Upper Layer Protocols (ULPs) that are used by applications to communicate over the InfiniBand network.
- **Switch**, connecting all the nodes in a switched point-to-point manner.
- **Fabric Management,** used to discover, bring up and manage all InfiniBand-based elements including switches and HCAs.
- **Gateway Modules**, providing connectivity to other network fabrics including InfiniBand, Ethernet and Fibre Channel.
- **Storage** (native and/or Fibre Channel access)
- **Device Management** is located on Voltaire Switches and enables users to configure and manage the device.

InfiniBand provides a reliable, low latency interconnect (with typical switch latency of 100nS) with fault-tolerance mechanisms (Automatic Path Migration), physical multiplexing (Virtual Lanes), physical link aggregation (1X and 4X) and security/partitioning.

The InfiniBand fabric provides central management and configuration controlling discovery, failures and resource allocation.

1.2 Scaling-Out Data Centers with QDR

Faster servers combined with high performance storage and applications that use increasingly complex models are causing data bandwidth requirements to spiral upward. As servers are deployed with next generation processors and server busses, high-performance computing environments - in industries such as energy, bioscience, financial services, government and academic research - will need every last bit of bandwidth delivered with Voltaire's new fourth generation Grid Director 4036 smart switches. As clusters grow in size and complexity, efficient routing, and advanced management tools become mandatory for quick fabric bring-up and minimal fabric down-time.

Voltaire's fourth generation InfiniBand switches add many new smart capabilities to meet the needs of next generation data centers. Smart switches are designed to fit easily into the modern data center's infrastructure with an optimized form factor.

1.3 4036 System Overview

The Voltaire Grid Director 4036 is a high performance, low latency and fully non-blocking InfiniBand switch for high performance clusters. Delivering 2.88 Tbps of non-blocking bandwidth with less than 100 nanoseconds of port-to-port latency, I/O bottlenecks are removed making applications operate at maximum efficiency. The Voltaire Grid Director 4036 has thirty-six 40Gbps ports that use the new smaller and intelligent QSFP connector in a 1U chassis that is only 15" deep. The efficient Grid Director 4036's smart design makes it easy to build clusters that can scale-out to thousands of nodes.

The Voltaire Grid Director 4036 also comes with new smart capabilities:

- The Grid Director 4036 includes smart device management that provides a simple interface for deploying, troubleshooting, maintaining and upgrading the switch. With a simple to use CLI interface, routine tasks such as monitoring the switches operation or upgrading software and firmware are made simple.
- With the increased 40Gbps speeds comes faster signaling rates. Voltaire's smart switch design leverages advances in cabling technology in concert with the Grid Director 4036's advanced port and signal optimization capabilities to determine the optimal settings for the connected QSFP cable. This makes the selection of cables more flexible and provides for simpler and faster cluster deployments without errors caused by degraded signal integrity.
- The Voltaire Grid Director 4036 comes with an onboard subnet manager, enabling simple, out-of-the-box fabric bring up, for small to medium clusters. Furthermore, the Grid Director 4036 can be coupled with Voltaire's Unified Fabric Manager (UFM), which automatically discovers, virtualizes, monitors and optimizes the fabric infrastructure and accelerates the active applications. UFM provides fast fabric bring-up by implementing leading-edge routing algorithms that maximize the use of available fabric bandwidth and enable the creation of scale-out clusters from tens to thousands of nodes.
- Applications require fabrics to provide reliable bandwidth and latency that can scale to support thousands of nodes. Voltaire fabric optimization includes advanced congestion management capabilities for detecting congestion with advanced multi-path and adaptive routing capabilities to prevent degraded application performance.

1.4 2036 System Overview

The Voltaire Grid Director 2036 is a high performance, low latency and fully non-blocking InfiniBand switch for high performance clusters. Delivering 1.44 Tbps of non-blocking bandwidth with less than 100 nanoseconds of port-to-port latency, I/O bottlenecks are removed making applications operate at maximum efficiency. The Voltaire Grid Director 2036 has thirty-six 20Gbps ports that use the new smaller and intelligent QSFP connector in a 1U chassis that is only 15" deep. The efficient Grid Director 2036's smart design makes it easy to build clusters that can scale-out to thousands of nodes.

1.5 4036/2036 Functional Block Diagram

Figure 1-1 below shows the 4036/2036 functional block diagram.

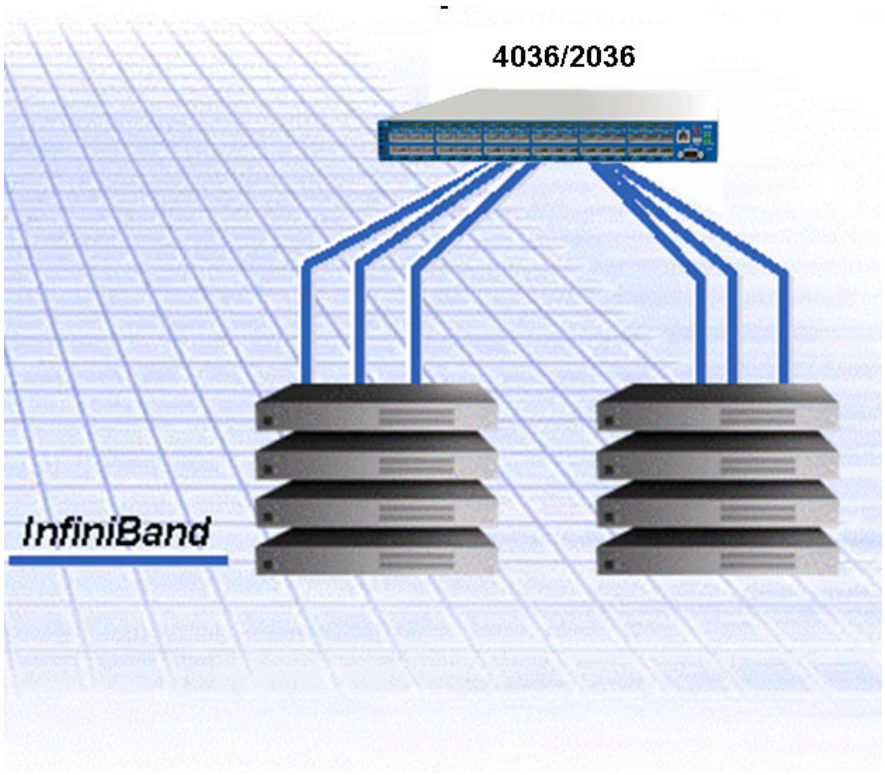

Figure 1-1. Voltaire 4036/2036 Grid Director Functional Diagram

1.6 Voltaire Switch Management

Management of Voltaire switch models is based on Voltaire's Grid Interconnect Management Software. The Voltaire Device management software is a powerful and comprehensive application that simplifies the management and proactively maximizes the performance and availability of InfiniBand enabled servers, networks, and storage grid environments.

The Voltaire Device Manager provides an embedded management functionality running under an InfiniBand switching platform.

The Subnet Manager automatically discovers the fabric topology, configures the hosts, and switches for ease of operation.

Voltaire switches can also be managed with existing management systems using standard protocols like InfiniBand subnet management. The system collects performance statistics and environmental monitoring data.

In-band management is derived from the InfiniBand network. In addition, the Fabric can be managed in-band or out-of-band. Out-of-band management is performed by the means of the fast Ethernet or RS-232 (console) interface.

Out-of-band management is performed by the means of the Ethernet or RS-232 (console) interface.

1.6.1 4036/2036 Grid Director Out-of-Band Ethernet/IB Management

The 4036/2036 out-of-band management is performed by the means of the Ethernet or RS-232 (console) interfaces.

Out-of-Band management is defined as managing the network through the Ethernet port of the 4036/2036. When using out-of-band management, external user applications can be connected directly through a network through the local Ethernet subnet in order to manage the Switch.

1.6.2 Management Interfaces

Voltaire switches have the following management interfaces:

- The Fast interface (10/100 Ethernet) provides an interface to the CLI via a Telnet or an SSH session as well as an interface to. The Fast interface also provides the interface to a remote server for downloading new switch software versions and for uploading backup files. Remote configuration settings are made using either the CLI.
- The Serial interface (RS-232) provides an interface to the CLI. (Out of band interface)

► Refer to Chapter 3 for a full detail on how to setup your system.

2

Chapter 2. CLI Overview

In This Chapter:

This chapter introduces the CLI, which provides commands to perform all necessary management functions.

It includes information on the following topics:

► Refer to the *CLI Reference Section* (Part 2) for a comprehensive list of menus and commands.

2.1 Interfaces for CLI Connection

A CLI session can be established via a serial RS-232 connection to the switch, or by connecting a Telnet or an SSH session to the management interface.

► Refer to First-Time Configuration, on page 3-2 for further information.

2.2 Telnet/SSH Client Settings

When using a Telnet/SSH client to connect, run, and configure the Voltaire products, make sure to check the **Telnet New Line** Settings to avoid CR/LF problems. Each client has its own location for those settings.

For example, when using Putty to run a Voltaire product, enter the Putty configuration window and under Connection/Telnet, make sure that the **Return key sends Telnet New Line instead of ^M** Checkbox is disabled, as shown below.

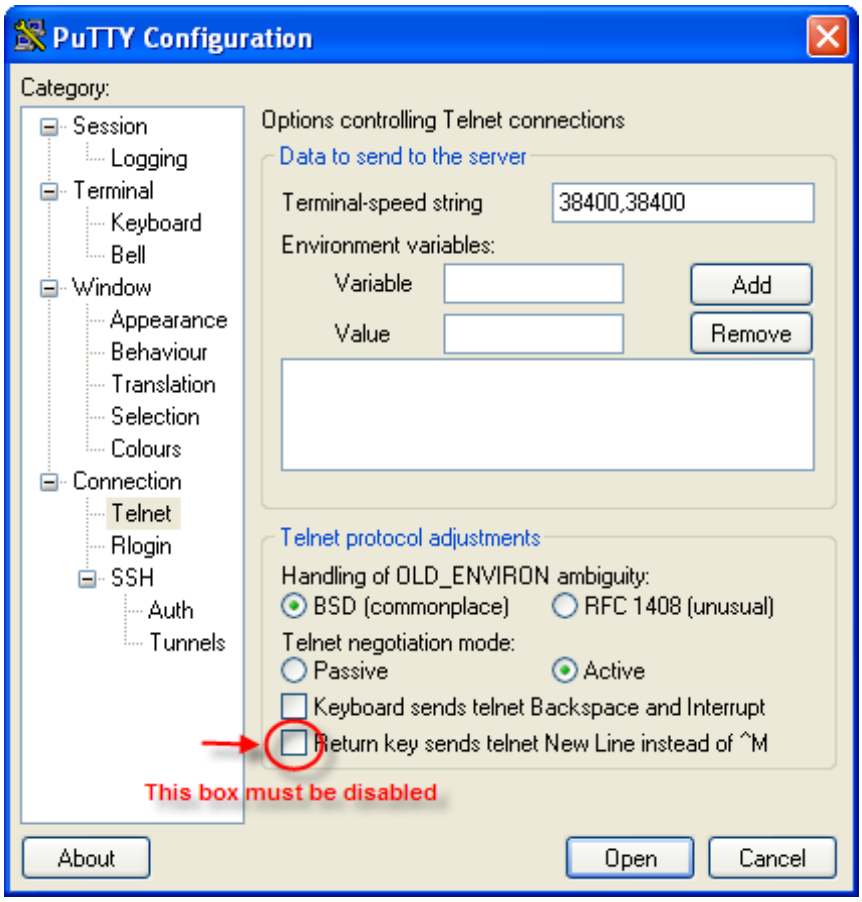

Figure 2-1. Telnet/SSH Client Settings – Example (using Putty)

2.3 CLI Usage Tips

- Automatic command completion
- Use the Tab key to complete commands as follows: type in the first one or few letters of the command and then key in Tab; the CLI completes the current word, allowing you to continue entering the command.
- Use the Question Mark (?) key to list all of the options available at that point in the command line.
- Commands and keywords can be truncated at any point after they are unique.
- The CLI is case sensitive. All commands and keywords must be entered in lower case; user-defined strings can appear in any case (including mixed case). Case for user-defined strings is preserved in the configuration.

2.4 Keyboard Usage in CLI Operation

The CLI supports the use of the following special keys for the described functions:

Table 2-1. CLI Key Functions

Key	Function
?	The question mark (?) key lists all of the options available at that point in the command line, along with a brief description of the command. If you enter a question mark (?) after a partial or complete command (use a space after the mark), the system provides a list of commands that begin with that string and relevant usage.
Tab	Completes a partial command name entry. When you enter a set of characters that match the beginning of a command name and press the Tab key, the system completes the command name. If you enter a set of characters that could indicate more than one command, the system lists all available options.
Backspace	Erases the character to the left of the cursor.
Return/Enter	At the command line, pressing the Return key performs the function of processing a command. At the prompt on a terminal screen, pressing the Return key scrolls down a line.

Key	Function
Left Arrow	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow key repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.
Right Arrow	Moves the cursor one character to the right.
Up Arrow or Ctrl-P	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down Arrow or Ctrl-N	Return to more recent commands in the history buffer after recalling commands with the Up Arrow or Ctrl-P. Repeat the key sequence to recall successively more recent commands.
Ctrl-A	Moves the cursor to the beginning of the line (**Note**: this button combo does not work when the session is established with Minicom).
Ctrl-B	Moves the cursor back one character.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Moves the cursor to the end of the command line.
Ctrl-F	Moves the cursor forward one character.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.
Ctrl-W	Deletes the word to the left of the cursor.
Ctrl-Y	Recalls the most recent entry in the delete buffer. The delete buffer contains the last ten items you have deleted or cut. Ctrl-Y can be used in conjunction with Esc Y.
Esc B	Moves the cursor from the middle of the word to the beginning.
Esc C	Capitalizes the character on which the cursor is pointing and moves it to the end of the word.
Esc D	Deletes from the cursor to the end of the word.

Key	Function
Esc F	Moves the cursor forward one word.
Esc L	Changes the word to lowercase at the cursor to the end of the word.

2.5 CLI Command Prompt

The CLI is password-protected. There are several CLI operation levels, each corresponding to a different level of interface operations. Each command mode requires a different password.

The CLI command prompt includes the switch name. Configuration changes are automatically saved as they are made. The > or # sign respectively show if you are in Exec (Admin) or Privileged configuration mode, as shown in the following table.

The following are the command modes:

- **guest** mode – Allows view-only access of switch configuration parameters
- **admin** mode – Allows the user to configure basic parameters such as date/time and reload (reset) switch, and to perform software and firmware updates
- **config** mode – Allows the user to configure all configuration parameters
- **debug** mode – Intended for use by Voltaire personnel only

The CLI command prompt includes the switch name. Configuration changes are automatically saved as they are made. The > or # sign respectively show if you are in guest or admin (Privileged) mode (which includes the utilities, config, and logs sub-menus), as shown in the following table.

Table 2-2. CLI Command Prompts

CLI Command Mode	Command Prompt	Access Method	Exit Method
guest	2036-xxxx> 4036-xxxx>	Log in	Use the **end** command.
admin	2036-xxxx# 4036-xxxx#	From the Guest mode, type **enable**. As an admin user, you enter directly into this mode.	To go back to Guest mode, type **disable** or exit. To enter config mode, type **config**.
config	2036-xxxx (config)#	From the Privileged mode,	To exit to Privileged mode, use the **exit** command or

CLI Command Mode	Command Prompt	Access Method	Exit Method
	4036-xxxx (config)#	use the **config** command.	the **end** command, which will exit the CLI.
debug	For use by Voltaire personnel only.		

2.6 CLI Command Structure

All CLI commands follow a simple structure, and are capable of prompting for further information as the user types. The following table lists the very basic CLI commands.

Table 2-3. Basic Commands

Command	Description
exit	Leaves current mode and return to previous mode.
?	Displays help text and usage for the Menu or CLI command.

<command>?	Displays help for the specific command.
	When typing "?" after a partial or complete command (use a space after the mark), the system provides a list of commands that begin with that string and relevant usage.
	To view the syntax, enter the whole command (by copying it) or simply type the first letter, space, and "?", as shown in the examples below:
	Example using the whole command:
	`4036-006E> firmware-version show ?`
	`firmware-version show  firmware-version show`

	The following shows the commands displayed by typing in the first word of the Command:
	`2036-0076# info?`
	`info-led set  info-led set [off, blink]`
	`info-led show  info-led show`
	The following shows the commands displayed by typing the first letter of the Command:
	`4036-006E# f?`
	`firmware-version show  firmware-version show`
	`front show  front show`

end	Terminates the current management session.

2.7 CLI Case Sensitivity

The CLI is case sensitive. All keywords must be entered in lower case. Any user-defined strings, such as names or descriptions, may appear in any case, including mixed case. Case information for user-defined strings is preserved in the configuration.

2.8 Built-in Test

When logging in Guest mode and before entering the CLI session, the Built-in Test runs several tests to verify the status of system processes and the direction of the fans.

This feature provides the ability to run scripts pre-defined by the CLI interface. You can also run this test manually from the Health Monitor sub menu. Note that this test runs automatically when logging into the CLI.

The Built-in test provides a report as shown below. If a test fails, it will be stated in the report.

Example:

```
login as: admin
admin@172.30.106.160 password:

Welcome to Voltaire Switch 4036

The built-in test will start in 5 seconds - press enter to skip the tests

Checking the status of system processes...      done
Checking the fan direction ...                  done
```

NOTE

There is a 5 seconds delay before the BIT starts running. You can skip the BIT by pressing the Enter key on your keyboard.

► Refer to the *CLI Reference Section* (Part 2) for a comprehensive list of menus and commands.

Chapter 3. Initial System Setup (CLI)

In This Chapter:

This chapter provides step-by-step instructions on how to setup your system, which is achieved via the Command Line Interface (CLI).

It includes information on the following topics:

3.1 Prerequisite Tasks

Before configuring system parameters, make sure you have completed the hardware installation according to the relevant Installation Guide.

Information about hardware installation of Voltaire switches can be found in the 4036/2036 Installation Manual.

3.2 First-Time Configuration

First-Time configuration is performed via CLI. The sections below describe the procedures for first-time configuration.

3.3 Collecting Required Information

Use the *Voltaire switch installation checklist* that follows to record the system and network information required for first time configuration.

The following information is required:

- Passwords – A password for users who will administer the switch.
  An additional password is needed to access the Privileged mode for advanced configuration. The default password for the Guest mode is **voltaire** and the password for the Admin (Privileged) mode is **123456**.

IMPORTANT

When entering the CLI or root for the first time, you are requested to change the factory default password for security reasons.

- Management interface IP address and subnet mask – The IP address and subnet mask of the Fast Ethernet interface (10/100 Ethernet).

Table 3-1. Switch Installation Checklist

System Parameter	Default
Guest mode password	password: `voltaire`
Privileged (enable) password (from the Guest mode)	password: `123456`
Management interface IP address Default management address: DHCP (enabled by default)	Default management IP address: DHCP. **Note: You must disable DHCP by running dhcp set disable before you can set the management IP address.** You can set the management IP address, as follows: `4036-006E(config-if)# ip-address set`

ip-address show	Determine if the management is set from the Ethernet or InfiniBand (Inband/outband management
	Example:
	`4036-006E(config-if)# ip-address show`
	`port selection Ethernet`
	`ip 172.30.106.160`
	`mask 255.255.0.0`
	`broadcast 172.30.255.255`
	`DHCP client disabled`
	`default-gw Ip is: 172.30.0.1`

`interface ethernet set` **OR**	Select this command if you want to set Ethernet as the Management interface.
`interface infiniband set`	Select this command if you want to set InfiniBand as the Management interface.
Subnet mask	255.255.255.0

Once you have completed the checklist, you are ready start the first time configuration of the switch.

3.4 Connecting a Console

Connect a PC with a terminal emulation program to the RS-232 console interface of the switch, as described in the *Voltaire 4036/2036 Installation Guide*. Make sure that the Switch terminal emulation program is configured as shown in the following table.

Table 3-2. Terminal Emulation Configuration

Setting	Value
Terminal Mode	VT-100
Baud	38400
Parity	No Parity
Stop Bits	1 Stop Bit
Flow Control	None

NOTE

Make sure that the minicom Serial Device is configured as follows /dev/ttyS0 or ttyS1, ttyS2. (ttyS0 is the name of serial device on the host that is connected to the switch via a minicom application. The last digit represents the physical position of the serial connector on the host. For example, if the host has only one serial connector, the device name should be /dev/ttyS0. If the host has 2 serial connectors, the device name could either be /dev/ttyS0 or /dev/ttyS1, and so on).

3.5 Starting a CLI Session

To start a CLI management session via serial connection to the switch:

Step 1 Connect the PC to the switch via its serial port, using the cable supplied by Voltaire.

Step 2 Start a HyperTerminal client (or compatible) on the computer.

Step 3 Configure the terminal emulation parameters as described in Table 3-2.

Step 4 When entering the CLI or root for the first time, you are requested to change the factory default password for security reasons.

The default root password must be during “first login”, namely during first login and more particularly, in the following situations:

- First log into the new system (with default definitions)
- First login after running the **factory-default** utility that sets default definitions of the system
- First login after software version upgrade that supports enforcing the change of the default root password on the first login from a version that does not support the feature.
- First login may be performed by the user logged in as **root** (to the fast IP or to both local IPs) in guest and admin (privileged) modes.

Step 5 Type the appropriate user name password at the logon prompt.

`guest`

a. Enter the guest mode. The default password for the guest user is `voltaire`.

b. Enter the Privileged mode as follows:

Type enable and enter the admin password (The default password for the admin user is `123456`.)

OR

`admin`

Enter directly the privileged mode.

The default password for the admin user is `123456`.

Step 6 Issue the appropriate CLI commands to complete the required actions.

3.6 Initial System Configuration for Management

3.6.1 Configuring the Management Interface IP Address

The system can be managed via either the Ethernet or the InfiniBand interfaces.

The switch must be configured with an IP address to allow remote management. Use the following table to enter the appropriate commands.

To configure the IP address:

	Command	Description
Step 1	`guest`	a. Enter the guest mode. The default password for the guest user is `voltaire`. b. Enter the Privileged mode as follows: Type `enable` and enter the `admin` password (The default password for the admin user is `123456`.) OR
	`admin`	Enter directly the privileged mode. The default password for the admin user is `123456`.
Step 2	`config`	Enters the **config** mode from the Privileged mode. Type the password when prompted.
	If the management is set to Ethernet, run: `dhcp set disable`	Disables dhcp (DHCP is enabled by default). When the management is set to Ethernet, you need to run `dhcp set disable` before running "ip-address set". In InfiniBand there is no need to run that command
Step 3	`interface`	Enters the interface configuration.
Step 4	`interface ethernet set` **OR**	Select this command if you want to set Ethernet as the Management interface.
	`interface infiniband set`	Select this command if you want to set InfiniBand as the Management interface.
Step 5	`ip-address set [ip-address] [netmask] [optional broadcast]`	Set the IP address of the selected interface. Example `4036-006E(config-if)#ip-address set 192.168.70.60 255.255.0.0`

	Command	Description
Optional	`Default gateway set`	Set the switch Default Gateway. Note that the default Gateway must be under the same subnet as the management interface Example `4036-006E( (config-if)#Default gateway set 192.188.0.1`

Optional	`ip-address show`	View the ip-address configuration.
		Example:
		`4036-006E(config-if)# ip-address show`
		`port selection Ethernet`
		`ip 172.30.106.160`
		`mask 255.255.0.0`
		`broadcast 172.30.255.255`
		`DHCP client disabled`
		`default-gw Ip is: 172.30.0.1`

Step 6	`exit`	Exits the **interface** mode to the **config** mode.

3.7 Time Settings

Time settings enable you to manually set the Switch internal clock using the procedure described in the following Section.

3.7.1 Manually Configuring Time and Date on your Switch

Use the following sequence to configure the switch time and date parameters. The time and date will appear on event reports that are time stamped.

To configure time and date on your switch:

	Command	Description
Step 1	`guest`	a. Enter the guest mode. The default password for the guest user is `voltaire`. b. Enter the Privileged mode as follows: Type `enable` and enter the `admin` password (The default password for the admin user is `123456`.) OR
	`admin`	Enter directly the privileged mode. The default password for the admin user is `123456`.

	Command	Description
Step 2	`config`	Enter the **config** mode
Step 3	`ntp`	Enter the NTP mode

Step 4	`clock set 010622002009`
	`clock show Sun Jan 6 22:00:11 UTC 2009`
		Enter time and date in military format, as shown in the syntax:
		`clock set MMDDhhmmYYYY[.ss]`
		Example:
		`clock set 042623192009`

Optional	`clock show` **Note:** this command is available under both the NTP and config menus)	View the system (switch) clock. Example: `Thu Apr 26 23:19:07 UTC 2009`

3.8 Configuring Passwords

Use the following procedure for configuring passwords for Exec and Privileged mode access to the RS-232 console interface and to the management interface (used for establishing a CLI session via Telnet or SSH).

NOTE:

The factory default password for the various modes are as follows:

guest: voltaire

admin: `123456`.

root: `br6000`

To configure passwords through the CLI, run the following commands:

	Command	Description
Step 1	`guest`	a. Enter the guest mode. The default password for the guest user is `voltaire`. b. Enter the Privileged mode as follows: Type `enable` and enter the `admin` password (The default password for the admin user is `123456`.) OR

	Command	Description
	`admin`	Enter directly the privileged mode. The default password for the admin user is `123456`.
Step 2	`password update [admin,enable,guest,root]`	Set the new passwords
Step 3	`exit`	Exits Privileged mode

Example:

```
4036-006E# password update admin
Insert new (up to 8 characters) password: [123456]
Please retype new password: [123456]
OK
```

3.9 Verifying Configuration

From the exec→privileged mode, verify the system parameters using the steps listed below. Note that the **ip-address show** command is available under the **config→interface** menu, under the **config** mode.

	Command	Description

Step 1	`version show`	Shows the version of the current switch software.
		Example:
		`4036-006E# version show`
		`ISR 2036/4036 version: 2.0.0`
		`date: Apr 07 2009 02:55:27 PM`
		`build Id:15`

Step 2	`remote show`	(Optional) Shows the Remote server configuration.
		Example:
		`4036-006E# remote show`
		`remote configuration`
		`----------`
		`remote server: 172.25.5.48`
		`username: root`
		`protocol: SCP`

	Command	Description

Step 3	`config→interface→ ip-address show`	Shows the IP interface address and configuration (Note that the ip-address show command is available under the config→interface menu).
		Example:
		`4036-006E(config-if)# ip-address show`
		`port selection Ethernet`
		`ip 172.30.106.160`
		`mask 255.255.0.0`
		`broadcast 172.30.255.255`
		`DHCP client disabled`
		`default-gw Ip is: 172.30.0.1`

Step 4	`config→clock show`	Shows the system clock.
		Example:
		`4036-006E# clock show`
		`Fri May 1 22:01:57 UTC 2009`

4

Chapter 4. Built-in-Test

In This Chapter:

This chapter provides details on the Built-in-Test and details the types of tests.

It includes information on the following topics:

4.1 Overview

The Built in test feature automatically performs several tests before entering the CLI session in Guest Mode. You can also run the tests manually from the Guest mode and the Privileged mode, under the Health Monitor sub-menu.

With this tool, you can run either one, several, or all scripts.

At the end of each test, the BIT shows that the test is done, whether it is successful or not.

In case of failure, an alert message follows immediately the failing test. In some cases, a troubleshooting option may be suggested.

Example at startup

```
#
4036-006E> bit all
Checking the status of system processes...      done
Checking the fan direction ...                  done
 ALERT: the fans direction doesn't match this system
```

4.2 Tests, Description and Explanations

Startup

All BITs are automatically executed during startup, as shown in the following examples. You can skip the BIT by pressing the enter key within 5 seconds:

```
#
4036-006E> bit all
Checking the status of system processes...      done
Checking the fan direction ...                  done
```

Running BIT Tests Manually

You can run a BIT from the Guest menu or from the Health Monitor Menu. The commands are detailed below.

bit

Description: Execute tests as part of Built in test. When logging in Guest mode, the Built in Test runs several tests before entering the CLI session. From this menu, you can choose the specific test that you want to run. This feature provides the ability to run any script was pre-defined by the CLI interface. You can also run this test manually from the Guest menu or the Health Monitor sub menu. Note that this test runs automatically when logging into the CLI.

When running a BIT, the BIT identifier is the number in the first column of the BIT show table (see following command)

- To execute all the tests, enter: `bit all`.
- To execute one or several BIT, type the test identifier separated by a comma (for example: 2, 5, 6). Note that you can run the BIT test in reverse order to, for example: bit 5, 1, 2 or in our example: bit 2, 1.
- To view the valid test list type show.

Syntax: `[test identifier, list of tests, all]`

Examples:

To execute one or more BITs:

1. Run a bit show command to view the test identifier:

```
4036-006E> bit-show
------------------------------------------------
BIT Identifier      Description
------------------------------------------------
1                   bit_tight_loop_check.sh
2                   bit_fan_direction_check
```

Note: Bit Show is detailed further below.

2. Select a bit identifier, for example #2:

```
4036-006E> bit 2
Checking the fan direction ...                  done
```

Note: All BITs are automatically executed during startup.

bit-show

Description: Shows all available built in tests with identifier and description.

Syntax: `bit show`

Example:

```
2036-005A> bit-show
-------------------------------------------------
BIT Identifier      Description
-------------------------------------------------
1                   bit_tight_loop_check.sh
2                   bit_fan_direction_check.sh
```

Test Description

```
Checking the status of system processes...      done
```

Checks that there are no processes in the switch that are in tight loop status.

Bit identifier: 1

Description: bit_ tight_loop_check.sh

```
Checking the fan direction...      done
```

Verifies that the fan air is flowing in the direction for the current configuration.

Bit identifier: 2

Description: bit_fan_direction_check.sh

5

Chapter 5. Updating, Backing up, and Upgrading the Software

In This Chapter:

This section explains how to configure switch parameters using CLI commands, including software upgrades and maintenance.

It includes information on the following topics:

5.1 Prerequisites

Before performing any switch maintenance tasks, make sure you have configured system parameters as described in First-Time Configuration, Section 3.2. Note that DHCP is **enabled** by default.

In addition, make sure that your remote server is set as described in the procedure below.

NOTE

Certain configuration tasks, such as identifying a location from which to download software, are optional, and may not have been performed during initial configuration. You may perform these tasks at any time via the CLI. Where necessary, this chapter will identify the relevant tasks and commands.

5.1.1 Setting the Remote Configuration Parameters for Backup

To set Remote configuration parameters and backing up the configuration:

Steps	CLI Command (Privileged Mode)	Description
Setting the Remote Configuration parameters		
Step 1	Switch(config-remote)# protocol set [FTP | SCP]	Sets the protocol to access remote server.
Step 2	Switch(config-remote)# remote show	Sets or shows the remote client configuration.
Step 3	Switch(config-remote)# username [username]	Sets the user name to access remote server.
Step 4	Switch(config-remote)# password [password] **Note:** Type <enter> before entering the password.	Edit password.

Steps	CLI Command (Privileged Mode)	Description
Viewing the configuration files		
	Switch(config-remote)# flash show	Shows the configuration files in flash.

5.2 Software Update

5.2.1 Overview

The switch is designed to run on a continuous basis without significant maintenance. However, from time to time, you may need to install updated software or modify device configuration. The switch stores a software image (along with configuration files, log files, and other information) on a local file system. This file system is stored on an internal flash memory.

The updated software is downloaded from a remote server (pre-defined by the user in the CLI Remote Menu).

The same software image can be used to manage any Voltaire Grid Director system. The software automatically detects the system type and executes the suitable device management operations.

The 4036/2036 has its own software image. The software automatically detects the system type and executes the suitable device management operations.

NOTE

Always review the README file before making updated software available to the switch.

If you plan to use the CLI `update software` command to update the switch software from a remote site, be sure to set the remote server IP address through the CLI Remote mode commands [Switch(config-remote)#] and make sure that the software version image is located on the Remote server.

- The software upgrade operation updates the entire boot image, and not individual components.
- A configuration merge is performed, as follows: old values are saved and new fields are added.

Once the user runs an update software command, the software is automatically updated.

The software upgrade procedure should last approximately ten to fifteen minutes.

5.2.2 Uploading the New Software/Firmware to the Remote Server

The new software and firmware update is available to the user either in media format (e.g. CD) or it from the Voltaire Support website. The user copies the update to a known location on a Remote server within the user's LAN.

The user defines the Remote parameters via the CLI config remote mode.

To upload the switch software and firmware, perform the steps listed below.

I. Copy the New Software Version to a pre-defined Remote Server

Note:

The Switch IP and the default Gateway must be configured prior to performing the following steps.

If a default gateway has not been configured, the Remote server must be located in the same subnet as the switch management port.

To upload the new software version to the remote server:

Step 1 Make sure that the Remote server is active.

Step 2 Copy the new version files to the Remote directory.

II. Configure Remote Server Settings

Identify the location from which to retrieve the updated software/firmware.

If this location is not the one from which you would normally retrieve updated software (using the switch management), use the steps in the following table to set the appropriate download location.

To configure the Remoter Server:

	Command	Description
Step 1	`guest`	a. Enter the guest mode. The default password for the guest user is `voltaire`. b. Enter the Privileged mode as follows: Type `enable` and enter the `admin` password (The default password for the admin user is `123456`.) OR

	Command	Description
	`admin`	Enter directly the privileged mode. The default password for the admin user is `123456`.
Step 2	config	Enter the **config** mode (from Privileged mode).
Step 3	remote	Access the Remote Mode (from the **config** mode)
Step 4	server [ip-address]	Configure the IP address of the Remote server.
Step 5	username [username]	Configure the user name for Remote server access.
Step 6	password	Set the user password to access the Remote server.
Step 7	protocol set [FTP | SCP]	Set the protocol to access remote server.
Optional	remote show	After the update is complete, execute this command to verify the new settings.

5.2.3 Switch Software Update

The update software command (in Privileged mode) updates the new switch software.

To update the Software:

	Command	Description
Step 1	`guest`	a. Enter the guest mode. The default password for the guest user is `voltaire`. b. Enter the Privileged mode as follows: Type `enable` and enter the `admin` password (The default password for the admin user is `123456`.) OR
	`admin`	Enter directly the privileged mode. The default password for the admin user is `123456`.
Step 2	version show	Check the current software version.

	Command	Description
Step 3	update software [update-file-dir]	Run this command to start the update software process. This can take several minutes to complete. Example `4036-006E#  update software RemoteDirectory`
		The system reboots. The system also updates the error log to notify the user if the update software was successful or not (for debugging purposes).

5.3 Firmware Upgrade

5.3.1 Overview

The 4036/2036 firmware runs on each InfiniBand switch ASIC. The firmware upgrade process detects the firmware in each ASIC and upgrades them.

Refer to the latest release notes for the relevant firmware image revision.

5.3.2 Functionality

Verification Functionality

The CLI (privileged mode/utilities menu) *firmware-version show* command is used to list and verify the firmware version and the PSID indicator for all the switch chips in the fabric.

Firmware Burning Functionality

The (privileged mode) *`update firmware`* CLI command supports burning the full chassis. The upgrade procedure can use the embedded firmware images as well external images retrieved via FTP.

Remote Firmware Upgrade

The (privileged mode) *`update remote-firmware`* is available for all switch platforms in the fabric, managed and unmanaged:

```
update remote-firmware [LID#,all] [update-file-dir]
```

The upgrade procedure updates the firmware version and can use the embedded firmware images as well external images retrieved via FTP.

5.3.3 Upgrade the Switch Firmware (Quick Steps)

The update firmware command (in Privileged mode) updates the local switch version of the firmware.

To update the new firmware version:

	Command	Description
Step 1	`guest`	a. Enter the guest mode. The default password for the guest user is `voltaire`. b. Enter the Privileged mode as follows: Type **`enable`** and enter the `admin` password (The default password for the admin user is `123456`.) OR
	`admin`	Enter directly the privileged mode. The default password for the admin user is `123456`.
Optional	`firmware-version show`	Verify the chassis PSID to see that you have the latest version installed. See examples in Section 5.3.4.
Step 2	`update firmware chassis [update-file-dir (if not present, takes local)]`	Use this command when there is new firmware to update on the local chassis. The firmware version is embedded in the new software. See examples in Section 5.3.

5.3.4 Firmware Image Identification (Verification Functionality)

The PSID is an indicator associated with each firmware image to allow firmware identification. The CLI (admin mode) *firmware-version show* command is used to list the firmware version and the PSID indicator for all the switch chips in the fabric. The following is and example of PSID format: VLT1150031011

You can view the PSID as detailed in the example below.

To view the firmware version and the physical parameter ID (PSID):

Step 1 From the CLI admin menu run the `firmware-version show` command to view the firmware version.

```
4036-006E# firmware-version show
FW Version:         7.2.0
PSID:               VLT1210030804
```

For more details regarding the upgrade procedure, refer to the following Sections on Software and Firmware Upgrade process.

5.3.5 Firmware Upgrade Process (Burning Functionality)

The upgrade procedure can use the embedded firmware images as well external images retrieved via the FTP or SCP.

To burn (update) the firmware, run the following command under the Privileged mode:

Step Run the following command:

```
4036-006E# update firmware chassis [update-file-dir (if not present, takes
local)]
```

This updates the chassis firmware version included in the software image.

Note: If you omit to specify the Remote Server address, the update firmware command will take the Grid Director image(s) from the local file system.

► The *CLI Reference Section* provides a comprehensive CLI reference detailing all the menus, commands, and usage.

6

Chapter 6. Handover Mechanism and Redundancy/High Availability

In This Chapter:

This chapter details the failover/handover and redundancy mechanisms:

6.1 SM (Subnet Manager) Handover

The main software running on the 4036/2036 Switch is the embedded Subnet Manager that configures the InfiniBand fabric and enables traffic flow.

The embedded SM implements the standard “SMInfo” protocol (IB Spec section 14.4) running in an InfiniBand subnet. The “SMInfo” protocol defines failover and handover between subnet managers in a given InfiniBand subnet in order to keep subnet configuration consistent even on failures.

SM priority between switches ranges between 1 and 15. This means that the SM with the higher priority is designated as Master and is the only SM that actively configures the fabric. You can change the SM priority and therefore change the master in the fabric.

Example:

If we have SM1 with priority 8 and SM2 with priority 9, SM2 becomes the Master SM and gets priority 9. In the CLI, the user can still change the priorities of the SM. Changing the priorities can result in handover, according to the priority policies.

All other SMs are in standby mode, polling the activity of the Master SM. In case of identical priorities between two switches in the same fabric, the switch with the lower GUID will become Master SM.

On Handover, mastership will be handed to the next prioritized StandBy SM by the priority-GUID rule and it will become the current Master.

An SM software malfunction will cause failover if there is another chassis in the fabric, according to the priority.

SM Priority Settings by the User

CLI:

You can manually set the SM priority (range 1-15) via the CLI using the following command (Note: you cannot perform a manual failover):

```
4036-006E(config-sm)#
sm-info priority set                sm-info priority set [int 1..15)]
```

6.2 Redundant Power Supplies

If a power supply fails, it turns red in the VDM and the problem or failure is displayed as an alarm (trap or event). For more information, refer to the Installation manual.

Power Supply mechanisms are hardware related and are detailed in the 4036/2036 Installation Manuals. The 4036/2036 supports two redundant Power Supplies.

6.3 Fans

If a fan fails and the system overheats, the system generates an error and event log.

Note that there is a thermal shutdown in case of overheating.

Fan mechanisms are hardware-related and are detailed in the 4036/2036 Installation Manual.

NOTE

The 6 fans in 4036/2036 are redundant. If one fails, the remaining fans shift to Turbo.

7

Chapter 7. 4036/2036 Device Manager

In This Chapter:

This chapter provides information about working with the 4036/2036 Device Manager CLI application.

This chapter includes information on the following topics:

7.1 Device Manager Overview

The Voltaire 4036/2036 Device Manager (VDM) is an embedded application that provides InfiniBand management functionality for the Voltaire 4036/2036 Grid Directors.

The Device Manager enables you to monitor and configure device parameters using the CLI.

Chassis temperatures as well as fan status are also provided.

7.2 4036/2036 - Obtaining Device Information

7.2.1 Viewing Device Information

You can view the device information by running the following commands.

Device Name

From the following CLI `Switch(config-names)#` menu, run the following command to see the Device Name (example).

```
4036-006E(config-names)# system-name show
system name is 4036-006E
```

Software Version

From the following CLI `Switch#` menu, run the following command to see the software version (example).

```
4036-006E# version show
ISR 2036/4036 version: 2.0.0
        date:    Apr 07 2009 02:55:27 PM
        build Id:15
```

Firmware Version

From the following CLI `Switch#` menu, run the following command to see the firmware version (example).

```
4036-006E# firmware-version show
FW Version:         7.2.0
PSID:               VLT1210030804
4036-006E#
```

7.3 Obtaining Detailed Information via the Device M

Detailed information can be obtained by running a front show command.

From the following CLI command (example), you can see the VPD (partial).

```
4036-006E> front show
Device:4036 Temperature: 25C normal
HW Version   : A02
Serial Number: AL4408000001
PS #1: PS fault
PS #2: ok
Num of fans: 6
Fans rate: normal
Fans direction: IN fault
Fan #1: ok
Fan #2: ok
Fan #3: ok
Fan #4: ok
Fan #5: ok
Fan #6: ok
The system DC power consumption is 38 W
```

The following table details the front show parameters.

Table 7-1. Information (Front Show) Parameters

Parameter	Description	Default/Range/Options
Temperature	Shows the device temperature	Temperature threshold: Relax (normal) =40 Warning = 60 Alarm = 80
HW Version	Shows the device hardware version	
Serial Number	Shows the device serial number	
PS #1	Shows the status of Power Supply #1	OK/PS Fault
PS #2	Shows the status of Power Supply #2	OK/PS Fault
Number of fans	Shows the number of fans that are operational in the system	6
Fans rate	Show the rate of the Fans	Normal/turbo
Fans direction	Shows the fan direction	IN/OUT fault
Fan #n	Shows the status of the specific fan	OK/Fan fault
DC power consumption	Shows the DC consumption	38 W

7.4 4036/2036 Local SM Information

The embedded SM on the 4036/2036 is active by default, and can be used to manage fabrics up to 648 nodes.

From the following CLI `Switch#` menu, run the following command to see the Local SM Information (example).

```
4036-006E# sm-info show
subnet manager info is:
sm routing_engine = minhop
sm sweep_interval = 15
sm max_wire_smps = 16
sm priority = 3
sm LMC = 0
sm max_op_vls = 5
sm transaction_timeout = 150
sm head_of_queue_lifetime = 16
sm leaf_head_of_queue_lifetime = 16
sm packet_life_time = 18
sm polling_timeout = 5000
sm polling_retry_number = 12
sm reassign_lids = disable
sm babbling_port_policy = disable
sm state = master
sm mode = enable
sm log_verbosity = verbose
```

Table 7-2. Local SM Information Parameters

Parameter	Description	Default
sm routing_engine	sm routing engine option: mimhop or updn	minhop
sm sweep_interval	The number of seconds between subnet sweeps (0 disables it)	15
sm max_wire_smps	Maximum number of SMPs sent in parallel	16
sm priority	SM priority used for deciding who is the master. Range goes from 0 (lowest priority) to 15 (highest).	4
sm LMC	The LMC value used on this subnet	0
sm max_op_vls	Limit the maximal operational VLs (see sm-info max_op_vls set for further detail)	5
sm transaction_timeout	The maximum time in [msec] allowed for a transaction to complete	150

Parameter	Description	Default
sm head_of_queue_lifetime	The code of maximal time a packet can wait at the head of transmission queue. The actual time is 4.096usec * 2^<head_of_queue_lifetime> The value 0x14 disables this mechanism	0x10
sm packet_life_time	The maximal time a packet can wait at the head of queue on switch port connected to a CA or router port.	0x10
sm polling_timeout	Timeout in [msec] between two polls of active master SM	5000
sm polling_retry_number	Number of failing polls of remote SM that declares it dead	12
sm reassign_lids	If enabled, causes all LIDs to be reassigned. (For more details, refer to the sm-info reassign_lids set command.)	disable
sm babbling_port_policy	Shows the Babbling Port Policy. For further details, refer to the sm-info babbling_port_policy set.	disable
SM Mode	Defines the SM functionality mode. Possible values are *Enable* or *Disable*.	enable
SM State	Read-only field that displays the current local SM state. Possible values are Standby, Master and Discovering. The SM can also be inactive. The Master shows that this SM is in master status. The other SM is in StandBy mode waiting for possible failover. Discovering means that before the SM is set as master or standby, it must first discover the network.	N/A
sm log_verbosity	Defines the verbosity mode of the SM log file. Possible values are listed from low to high verbosity, as follows: Error, Info, Verbose, Debug, Function, Frames.	Verbose

7.5 4036/2036 Temperature Information

When a device heats up (according to preset threshold defaults that cannot be adjusted by the user), the switch increases fan speed.

The fan speed also increases when one of the internal fans is faulty.

Temperatures are displayed both in Fahrenheit and in Celsius.

Default: Temperature threshold: Relax (normal) =40, Warning = 60, Alarm = 80

After a power cycle, the fan speed is initialized to turbo. If all the temperature sensors are below the warning threshold, the fan rate is set to Normal. If one of the temperature sensors is above the warning threshold, the Fan rate is set to turbo. If one of the Fan units is missing, the other unit is set to Turbo. If one of the Fan trays or one Fan in the unit is failing, all the other Fans are set to Turbo.

Each device has three temperature thresholds:

- RELAX threshold
- WARNING threshold
- ALARM threshold

After a successful scan of the sensors of the chassis, the fan speed is set to normal if sensors are below the WARNING threshold.

The system periodically scans the chassis. If any of the above condition fails, fan speed is set to turbo.

A thermal shutdown occurs when the temperature is above 70 degrees Celsius (158 degrees Fahrenheit).

To view temperature information and fan status, run the following command From the following CLI `Switch#` menu (example):

```
4036-006E# front show
Device:4036 Temperature: 27C normal
HW Version   : A02
Serial Number: AL4408000001
PS #1: PS fault
PS #2: ok
Num of fans: 6
Fans rate: normal
Fans direction: IN fault
Fan #1: ok
Fan #2: ok
Fan #3: ok
Fan #4: ok
Fan #5: ok
Fan #6: ok
The system DC power consumption is 40 W
```

You can view the temperature per sensor by running a `4036-006E# temperature show` command, as shown below.

```
4036-006E# temperature show
Temperature sensor #0[normal (T=<36)]: 26[C], 78[F]
Temperature sensor #1[normal (T=<36)]: 25[C], 77[F]
Temperature sensor #2[normal (T=<36)]: 26[C], 78[F]
Temperature sensor #3[normal (T=<36)]: 27[C], 80[F]
```

Table 7-3. Temperature Show Parameters

Parameter	Description	Default
Temperature sensor n	Shows the temperature of the specific sensor. There are four sensors. [C] shows the actual temperature in centigrade. [F] shows the actual temperature in Fahrenheit.	Temperature range: Normal should be under 36 degree centigrade.

7.6 4036/2036 Reset

You can reset the 4036/2036 software using the CLI by using `4036# reload` command to reboot the 4036/2036; this command is required after performing various software operations in order for configuration changes to take effect.

Using the CLI, you can reset the 4036/2036 software. Run the following command to reset the software.

From the following CLI `Switch#` menu, run the following command to reload the chassis:

```
4036-006E# reload
```

When prompted, confirm if you want to reload the chassis.

This command is required after performing various software operations in order for configuration changes to take effect. This is a software reset.

7.7 Viewing the Event and Error Log

This log is used to view the errors that occur within the system. It is used for diagnostic purposes.

You can view the Error Log by uploading the ExportLog to a remote server and viewing the log, as described below.

To view the Error Log via the CLI:

Step 1 Run the following command `Switch(config-remote)# exportLOGs` command. This uploads the Logs to the remote server, using previously defined server name, user name, and password. These logs include the error logs.

Step 2 Access the file on the remote server to view the errors in the log.

Refer to the CLI Logs Mode, in section 18.5, for a list of all the log types, their descriptions, and the CLI commands you need to run to obtain them.

8

Chapter 8. Remote Configuration Settings

In This Chapter:

This chapter provides instructions on how to configure your remote server. It includes information on the following topics:

8.1 Overview

The FTP/SCP functionality is used to:

- Upgrade software versions
- Upload log files to the remote server
- Upload→ download the repository file

NOTE:

All operations below can be performed via both FTP and SCP

8.2 Setting the Remote Configuration Parameters

To set Remote configuration parameters and backing up the configuration:

Steps	CLI Command (Privileged Mode)	Description
Setting the Remote Configuration parameters		
Step 1	Switch(config-remote)# protocol set [FTP | SCP]	Sets the protocol to access remote server.
Step 2	Switch(config-remote)# remote show	Sets or shows the remote client configuration.
Step 3	Switch(config-remote)# username [username]	Sets the user name to access remote server.
Step 4		Indicates the remote path in which the transferred file will be created.
Step 5	Switch(config-remote)# password [password]	Edit password.

Steps	CLI Command (Privileged Mode)	Description
Backing up the configuration		
Step 1	Switch(config-remote)# flash show	Shows the configuration files in flash.
Optional	**Switch(config-remote)#copy running-config: remote:** copy running-config remote: [remote-path]	Uploads the configuration to the remote server using previously defined server name, user name, and password. The remote path can contain the imported file name. If the file name is not indicated, it will be created using a default name. Any characteristic after the last slash in the path will be used as a user-defined file name.
Optional	**Switch(config-remote)#copy remote: running-config** copy remote: [remote-path] running-config	Downloads the configuration from the remote server using previously defined server name, user name, and password. The remote path must contain the exported file name. The new values will be applied on reboot.
Optional	**Switch(config-remote)#copy running-config flash:** copy running-config flash: [file-name]	Backs up the configuration into file in the local repository. In case of empty name the file name is set by default (example of default format: repository_ISR2004-38fa_6_47_2008-01-21_IP_172.30.106.32.new). You can back up to two files. Backing up additional files will prompt a message that you are over the limit. Note that the chassis can store up to two local flash files simultaneously under different names.

Steps	CLI Command (Privileged Mode)	Description
Optional	**Switch(config-remote)#copy flash: running-config** copy flash: [file-name] running-config	This restores the backup configuration. This command retrieves the repository configuration from a file stored in the Flash, restores it and saves it in the switch repository (database). The new values will be applied on reboot.
Optional	Switch(config-remote)#flash delete	Deletes the specific repository file from flash. Note that the chassis can store up to two local flash files simultaneously under different names.

Refer to Section 00 for the list of Remote commands provided by the CLI.

9

Chapter 9. Security Settings

In This Chapter:

This chapter provides information on how to use the system features to set system (chassis) security. It includes information on the following topics:

9.1 Overview

InfiniBand architecture defines an infrastructure delivers performance and latency and enhanced datacenter security compared with standard high-performance networks.

Security is usually categorized into confidentiality, access control, authentication, and data integrity.

This section introduces the Grid Directors security mechanisms.

Voltaire provides security for its Switch implementing secure protocols (SCP) and disabling telnet. In addition, it enables encryption via the SSH and SCP protocols.

IMPORTANT:

Your system is delivered without security. (telnet and ftp are enabled by default).

Set up your system according to your security needs by using the following commands.

Access Control and Authentication for Switch Management

1. User Authentication (local and remote)
2. Disable access non-secured protocols (Telnet)

Encryption

- SSH Protocol (Secure Shell) – (telnet/SSH)
- SCP Protocol

9.2 SCP - Secure Export and Import

9.2.1 Overview

Secure export and import of files and software upgrades between computers is achieved using SCP (Remote Secure Copy Protocol). SCP is a secure form of FTP, to which it is similar. SCP is itself based on the SSH protocol, which provides the enhanced security.

Each of SCP and FTP possesses some advantages not found in the other. E.g., SCP provides upload of certain file properties that FTP does not. On the other hand, FTP can transfer also directory information whereas SCP can transfer only files.

Voltaire provides two forms of remote file and directory access: FTP and SCP. These two protocols are packaged as a single 'remote mode' command set available through CLI.

9.2.2 SCP Settings

To set SCP:

Step 1 From the CLI→config→remote mode, set the SCP status, as follows:

Example:

```
Switch(config-remote)#protocol set SCP
```

Step 2 View the Remote status, as follows.

Example:

```
Switch(config-remote)# remote show
remote configuration
----------------------
remote server: 172.25.5.48
username:      root
protocol:      SCP
```

9.3 Enabling/Disabling Non-secure Protocols

9.3.1 Disabling Telnet Access

The telnet daemon provides the server function for the telnet protocol.

The telnet features enables you to access the switch from a remote site. Telnet is less secure than SSH and in order to enhance security, it is recommended that you disable the telnet daemon as described below.

Note: Telnet is enabled by default.

To set telnetd via the CLI:

Step 1 From the CLI→config→security menu, set the telnetd status, as follows:

Example:

```
4036-006E(config-security)# telnetd set disable
```

Step 2 View the telnetd status, as follows.

Example:

```
4036-006E(config-security)# telnetd show
telnetd       disable
```

Refer to Section 19.90 for the list of Security commands provided by the CLI.

10

Chapter 10. Unified Fabric Manager Support

The UFM agent is an embedded tool that enables the UFM to discover the system and fabric management.

If you have UFM, these commands allow you to enable/disable the UFM agent software running on the switch. This agent can only be used if the UFM software is installed on a host in the fabric.

The UFM agent provides the UFM server with information about the switch parameters, such as IP address, GUID, etc. over Ethernet. It is using the TCPIP protocol and is listening to the port 8000.

NOTE

ufmagent is enabled by default. Enabling or disabling the ufmagent will take effect after reloading the switch.

ufmagent CLI options

---

ufmagent set

Description: Disables or enables the ufm agent

Syntax: `ufmagent  set [enable|disable]`

Default: enable

Example:

```
4036-006E(config-security)# ufmagent  set disable
Change will be effective only after next reboot
```

ufmagent show

Description: Shows the ufm agent

Syntax: `ufmagent show`

Example:

```
4036-006E(config-security)# ufmagent  show
ufmagent mode is disable
```

Refer to Section 19.9 for the list of UFM agent commands provided by the CLI.

Refer to the Unified Fabric Manager (UFM) User Manual for more information on the UFM manager.

11

Chapter 11. Factory Defaults

Factory default reverts the 4036/2036 to its factory default parameter settings and reloads the system. Since this command restores the switch default interfaces IP address, it is important to perform this action via a local terminal in order not to lose communication with the switch.

Running the factory default will erase all non-default data.

To set factory default, run the following command from the config menu:

```
4036-006E(config)# factory-default
```

Refer to Chapter 19 for the CLI command and description related to this topic.

12

Chapter 12. QSFP Port Management

The Ports menu allows to disable or enable QSFP ports (ports are enabled by default). Ports can be disabled if you want to block it for maintenance or they are faulty.

NOTE

This configuration is not persistent (it needs to be set again after reboot).

The following are the commands available under the Port menu.

```
4036-0076(config-port)# ?
<command> ?     Displays the command usage string
?               Displays the list of available commands
end             Ends the CLI
exit            Exits to previous menu
port set        Enables/disables port.
port state show Shows the port's physical and logical states
```

Port syntax usage is as follows:

```
port set        port set [enable | disable] [port num (1-36)]
port state show port state show
```

To set port configuration, run the following commands available under the config-Port menu.

port set

Description: Enables/Disables the selected port(s)

Syntax: `port set [enable | disable] [port num (1-36)]`

Default: `enable`

Example:

```
4036-0076(config-port)# port set disable 1
```

Expected results are shown in the following command (port down).

NOTE:

This **port set configuration** is not persistent after reboot.

port state show

Description: Shows the state of the specific port

Syntax: `port state show [port num (1-36)]`

Example:

```
2036-0076(config-port)# port state show 2
logical state = down
physical state = polling
```

Refer to the CLI Ports Mode, section 19.6, for more information on port configuration.

13

Chapter 13. Configuring the Subnet Manager

The InfiniBand Subnet Manager (SM) is a centralized entity running in the switch. It discovers and configures all the InfiniBand fabric devices to enable traffic flow between those devices.

The SM applies network traffic related configurations such as QoS, routing, partitioning to the fabric devices.

You can view and configure the Subnet Parameters (SM) via the CLI `(config-sm)` menu. This section describes how to view and configure the SM parameters.

Refer to Section 0 for the list of routing algorithms provided by the CLI.

14

Chapter 14. Configuring Routing Algorithms

In This Chapter:

This chapter provides instructions on how to configure routing Algorithms.

It includes information on the following topics:

14.1 Supported Algorithms

The 4036/2036 supports the following routing algorithms:

- Balanced-routing
- Up-down routing

14.2 Min Hop (Balanced Routing) Scheme

This is the default routing scheme and is applicable to all Fabric configurations. InfiniBand routing is done in the following manner: each InfiniBand switch maintains a simple forwarding database that defines, per destination LID, which physical port should be used for outgoing packets. The forwarding databases are configured by the Subnet Manager when the subnet is initially configured and upon network changes.

In the event that multiple paths exist between a pair of nodes in the subnet, the Subnet Manager identifies multiple minimal paths among those end-ports, selects one path and programs the fabric accordingly. However, to better utilize network bandwidth, the Subnet Manager balances its selections such that the traffic between all end-ports is balanced over all possible paths in the fabric.

14.3 Up/Down Routing Scheme

Up-Down routing is designed for CLOS networks.

The algorithm objective is to assure that given an N-stage CLOS network, each lid route between a couple of end-ports passes through the CLOS backbone level (i.e., the spine level). The path from the source end-port up to the back-bone level is called up route, and the remaining path from the back-bone level till it gets to the destination end-port is called down route.

To ensure optimal performance in 5-stages CLOS network, it is recommended to use the up-down routing

The up-down algorithm eliminates the hazard of credit loops for a CLOS network.

NOTES:

There is an exception to that rule, in the case where there exist a route of length<N between those two end ports. In that case, the route should not go through the backbone level. For example, in a 3-stage CLOS network, if both end-ports connect to the same switching chip on the first level of the CLOS, then the route should not traverse the CLOS backbone level.

14.4 Setting the Routing Algorithm

To set the routing algorithm, run the following command from the (config-sm)# prompt:

sm-info routing_engine set

Description: Sets routing_engine SM parameter. The sm-info routing_engine set sets the routing algorithm to be implemented by the Subnet Manager. The Voltaire Subnet Manager supports the following routing algorithms:

- Up-down algorithm
- Min Hop (Balanced-routing)

Syntax: `sm-info routing_engine set [updn, minhop]`

Options: `updn, minhop`

Default: `minhop`

Example:

```
4036-0076(config-sm)# sm-info routing_engine set updn
```

Refer to Section 0 for the list of routing algorithms provided by the CLI.

15

Chapter 15. Utilities

The 4036/2036 CLI provides a comprehensive list of utilities enabling you to view the all switches, routers, and/or hosts in the fabric and obtain detailed device and port information. The 4036/2036 utilities provide enhanced diagnostic functionality.

Refer to Section 18.6 the full list of utilities, descriptions, and examples.

PART 2:

CLI Reference Section

This section explains the CLI basic concept, details the CLI command menus and command syntax, and provides examples for each command. The CLI provides configuration and management functions for Voltaire switches, as well as a wide range of provisioning, configuration and maintenance functions for the InfiniBand fabric. Access via the CLI is important for advanced and detailed configuration and troubleshooting.

This CLI Reference section covers the 4036/2036 CLI commands.

NOTE:

CLI commands and examples displayed in this document were randomly taken from either the 4036 or the 2036 Grid Director switches or from the Grid Switch. These representations are generic and are applicable to either switch, unless stated otherwise.

CAUTION:

Do not use root permissions for the Voltaire switches. Use of root permission for the switches is at the user's own risk.

You will get the following message if connecting as root:

```
login as: root
root@172.30.106.124's password:
You have logged in with root access.
Operations available in this mode may affect the system normal
operation and should only be performed after you get the approval from
your Support Representative.
```

16

Chapter 16. Getting Started with the CLI and Top Level Structure

In This Chapter:

This chapter refers to the Getting Started Overview and Initial Setup and provides a quick list of the CLI Menus and Commands.

16.1 CLI Overview

Chapter 2 provides an Overview of the CLI. It provides the following details:

- Interface for CLI connection
- Telnet/SSH Client Settings
- CLI Usage Tips
- Keyboard Usage an CLI Operation
- CLI Command Prompt
- CLI Command Structure
- CLI Case Sensitivity
- An Introduction to Built-in Test

16.2 CLI Initial Setup

Refer to Chapter 3 for details on how to set up the CLI for the first time. This chapter includes details on:

- Prerequisites
- First-time configuration
- Collecting required information
- Connecting a console
- Starting a CLI Session
- Initial system configuration for management and configuring the management interface IP address.
- Time settings
- Configuring passwords
- Verifying configuration.

16.3 CLI Structure

The Voltaire CLI concept implements a hierarchical organization.

The following command groups are available in the CLI:

Guest Mode	**Admin Mode**
Read-only Menu	**Admin Login: admin**
Administrator Login: admin	**Password: 123456**
Password: 123456	**(Note: The admin user enters this mode)**
Guest Login: voltaire	**Login: enable (from the Guest mode)**

config Sub-Menu		**SM Sub-Menu**	
factory-default	19-37	sm-info babbling_port_policy set	19-58
interface	19-37	sm-info head_of_queue_lifetime set	19-59
names	19-37	sm-info leaf_head_of_queue_lifetime set	19-59
port	19-37	sm-info lmc set	19-60
remote	19-38	sm-info max_op_vls set	19-60
security	19-38	sm-info mode set	19-61
sm	19-38	sm-info packet_life_time set	19-61
		sm-info polling_retry_number set	19-61
		sm-info priority set	19-62
		sm-info reassign_lids set	19-63
		sm-info routing_engine set	19-63
		sm-info show	19-63
		sm-info sminfo_polling_timeout set	19-64
		sm-info sweep_interval set	19-64

The following sections provide a detail of each mode and commands.

17

Chapter 17. Guest Mode

In This Chapter:

When a CLI session is started on the switch, the user enters the Guest mode which allows view-only access of switch configuration parameters.

This chapter lists the commands in the Guest Mode Commands Reference and contains the following sections:

17.1 Accessing the Guest Mode

`Guest login`	a. Enter the guest mode. The default password for the guest user is `voltaire`. b. Enter the Privileged mode as follows: Type enable and enter the admin password (The default password for the admin user is `123456`.) OR
`Admin login`	Enter directly the privileged mode. The default password for the admin user is `123456`.

You can type exit to exit this mode (and the CLI).

NOTE:

The > prompt shows that you are in Guest Mode.

The following example shows how to access the guest mode. As soon as you enter the guest mode, the Built-in test checks the health of the system.

Example:

```
login as: guest
guest@172.30.106.124's password:
The built-in test will start in 5 seconds - press enter to skip the tests
0
Checking the status of system processes...      done
Checking the fan direction ...                  done
```

17.2 Guest Mode Command Reference

The commands available in the Guest mode and their descriptions are listed below.

NOTE:

The > prompt shows that you are in Guest Mode.

```
4036-006E> ?
<command> ?             Displays the command usage string
?                       Displays the list of available commands
bit                     Executes tests as part of built in test procedure
                        Executes all the tests by typing all
                        Executes one or several tests by typing the test
                        identifiers separated by comma (for example: 2,5,6)
bit-show                Shows all available built-in-tests with identifier
                        and description
cable-config show       Shows the cable configuration
clock show              Shows the system clock
enable                  Change to PRIVILEGED mode
end                     Ends the CLI
exit                    Exits to previous menu
firmware-version show   Shows firmware version information
front show              Shows the blade module information at the front
                        of the chassis
ping                    Sends ping messages
remote show             Shows the remote client configuration
route default-gw show   Shows the default gateway IP address
sm-info show            Shows the Subnet Manager (SM) parameters
temperature show        Shows the board temperature in Celsius and
                        Fahrenheit
version show            Shows the software version information
```

The following details the commands available in Guest mode:

<command> ?

Description: Displays a brief help text on the specified command.

Syntax: `<command> ?`

?

Description: Displays a list of available commands in the current CLI mode/menu.

Syntax: `?`

bit

Description: Execute tests as part of Built in test. When logging in Guest mode, the Built in Test runs several tests before entering the CLI session. From this menu, you can choose the specific test that you want to run. This feature provides the ability to run any script was pre-defined by the CLI interface. You can also run this test manually from the Health Monitor sub menu.

Note that this test runs automatically when logging into the CLI.

When running a BIT, the BIT identifier is the number in the first column of the BIT show table (see following command)

To execute all the tests type: `bit all`.

To execute one or several BIT, type the `test identifier` separated by a comma (for example: bit 1,2,3).

To view the valid test list type `bit-show`.

Syntax: `bit [test identifier, list of tests, all]`

Parameters: `Test identifier`: a single test

`List of tests`: test list using the selected test identifiers

`All`: list of all the tests

Examples:

To execute one or more BITs:

1. Run a bit show command to view the test identifier:

Example:

```
4036-006E> bit-show
-------------------------------------------------
BIT Identifier      Description
-------------------------------------------------
1                   bit_proc_tight_loop_check.sh
2                   bit_fan_direction_check
```

Note: Bit Show is detailed further below.

2. Select a bit identifier, for example BIT #2:

```
4036-006E> bit 2
Checking the fan direction ...                  done.
```

All BITs are automatically executed during startup, as shown in the examples below:

Expected Results:

```
login as: guest
guest@172.30.106.124's password:
The built-in test will start in 5 seconds - press enter to skip the tests
0
Checking the status of system processes...      done
Checking the fan direction ...                  done
```

bit-show

Description: Shows all available built in tests with identifier and description.

Syntax: `bit [test identifier, list of tests, all]`

Example - Grid Switch:

```
4036-006E> bit-show
-------------------------------------------------
BIT Identifier      Description
-------------------------------------------------
1                   bit_proc_tight_loop_check.sh
2                   bit_fan_direction_check
```

Example: Viewing specific tests using the BIT command

Use the test identifier listed in bit-show to run a specific test (using the BIT command, detailed in the previous command)

```
4036-006E> bit 2
Checking the fan direction ...                  done.
```

<command> ?

Description: Displays a brief help text on the specified command.

Syntax: `<command> ?`

cable-config show

Description: Shows the cable configuration. The system is able to automatically detect cable information if it is available.

Cable is not present – no cable in installed in this port.

Cable is present – a cable is installed in this port but no cable information is available.

Cable information – a cable is installed in this port and the cable information is detailed.

Cable error – error reading the cable information.

Supported cables – For the list of supported cables, refer to the 4036/2036 Installation Manual.

Syntax: `cable-config show`

Example:

```
4036-006E> cable-config show
```

```
Port#  1: Not present
Port#  2: Not present
Port#  3: Not present
Port#  4: Not present
Port#  5: Not present
Port#  6: Not present
Port#  7: Not present
Port#  8: Not present
Port#  9: Not present
Port# 10: Not present
Port# 11: Not present
Port# 12: Not present
Port# 13: Not present
Port# 14: Not present
Port# 15: Not present
Port# 16: Not present
Port# 17: Not present
Port# 18: Not present
Port# 19: Not present
Port# 20: Not present
Port# 21: Not present
Port# 22: length 1 Vendor Name: WLGORE Code: QSFP Vendor PN: SCN-2012-9
Vendor Rev: P1 Vendor SN: 070108-060
Port# 23: Not present
Port# 24: Not present
Port# 25: Not present
Port# 26: Not present
Port# 27: Not present
Port# 28: Not present
Port# 29: Not present
Port# 30: Not present
Port# 31: Not present
Port# 32: Not present
Port# 33: Not present
Port# 34: length 1 Vendor Name: WLGORE Code: QSFP Vendor PN: SCN-2012-9
Vendor Rev: P1 Vendor SN: 070108-060
Port# 35: Not present
Port# 36: Not present
```

enable

Description: Changes to Privileged mode from the Guest mode. Note that the **admin** user enters directly the Privileged mode when logging in and does not need to run the enable command. For further information on Privileged mode, refer to Chapter 18. The privileged mode prompt is as follows: 4036-006E#

Syntax: `enable`

end

Description: Ends the CLI. Exits to login menu from any other mode via a console connection, closes a Telnet session via a Telnet connection or closes an SSH session.

Syntax: `end`

exit

Description: Exits to previous menu. When in **guest** mode, this command is equal to the 'end' command prompting you to exit the CLI.

Syntax: `exit`

firmware-version show

Description: Shows the firmware version information and the relevant PSID>

Syntax: `firmware-version show`

Example:

```
4036-006E> firmware-version show
FW Version:         7.1.948
PSID:               VLT1220030706
```

front show

Description: Shows the blade module information as it appears at the front of the chassis including device idenfication, temperature, hardware version, serial number, power supply statuses, number of internal fans, fan direction, fan rate, and overall power consumption of the device.

Syntax: `front show`

Example:

```
4036-0076# front show
Device:2036 Temperature: 45C normal
HW Version   : A02
Serial Number: AL4608000120
PS #1: ok
PS #2: ok
Num of fans: 6
Fans rate: normal
Fans direction: IN fault
Fan #1: ok
Fan #2: ok
Fan #3: ok
```

```
Fan #4: ok
Fan #5: ok
Fan #6: ok
The system DC power consumption is 38 W
```

ping

Description: Sends ping messages to network hosts. Pings a specified network host up to four times. Press Ctrl-C to stop pinging.

Syntax: `ping <IP address>`

Example:

```
4036-006E> ping 172.30.106.30
PING 172.30.106.30 (172.30.106.30): 56 data bytes
64 bytes from 172.30.106.30: icmp_seq=0 ttl=64 time=0.2 ms
64 bytes from 172.30.106.30: icmp_seq=1 ttl=64 time=0.1 ms
64 bytes from 172.30.106.30: icmp_seq=2 ttl=64 time=0.1 ms
64 bytes from 172.30.106.30: icmp_seq=3 ttl=64 time=0.1 ms

--- 172.30.106.30 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
```

remote show

Description: Shows the remote client configuration.

Syntax: `remote show`

Example:

```
4036-006E> remote show
remote configuration
----------------------
remote server: 172.25.5.48
username:      root
protocol:      SCP
```

route default-gw show

Description: Shows the default gateway IP address.

Syntax: `route default-gw show`

Example:

```
4036-006E> route default-gw show
default-gw is: 172.30.0.1
```

sm-info show

Description: Returns the parameter settings of the Switch Subnet Manager.

Syntax: `sm-info show`

Example:

```
4036-006E> sm-info show
subnet manager info is:
sm routing_engine = ftree
sm sweep_interval = 20
sm max_wire_smps = 5
sm priority = 10
sm LMC = 6
sm max_op_vls = 5
sm transaction_timeout = 240
sm head_of_queue_lifetime = 10
sm leaf_head_of_queue_lifetime = 10
sm packet_life_time = 10
sm sminfo_polling_timeout = 1100
sm polling_retry_number = 100
sm reassign_lids = disable
sm babbling_port_policy = disable
sm state = discovering
sm mode = enable
```

NOTE:

Refer to Section 0 for a description of the Subnet Manager parameters.

temperature show

Description: Shows the board temperature in Celsius and Fahrenheit and their relavtive status..

Syntax: `temperature show`

Default: Temperature threshold:

Warning = 60

Alarm = 80

Relax (normal) =40

Example:

```
4036-006E> temperature show
Temperature sensor #0[alarm (T>=30)]: 41[C], 105[F]
Temperature sensor #1[alarm (T>=30)]: 41[C], 105[F]
Temperature sensor #2[alarm (T>=30)]: 41[C], 105[F]
```

```
Temperature sensor #3[alarm (T>=30)]: 42[C], 107[F]
```

version show

Description: Displays the software version information and the date the software was burned.

Syntax: `version show`

Example:

```
ISR 2036/4036 version: 2.0.0
        date:    Feb 15 2009 08:39:54 AM
        build Id:1000
```

18

Chapter 18. Admin Mode

In This Chapter:

This chapter provides the commands available under the privileged mode and contains the following sections:

18.1 Overview

The Admin (Privileged) mode command is used to configure basic parameters such as date/time, reload (reset) switch, and perform software and firmware updates.

Admin users log directly into the privileged mode using the admin default password: `123456`.

In order to access the privileged mode, the Guest user must type “enable” at the prompt and enter the admin password: `123456` (admin default password).

18.2 Accessing the Admin (Privileged) Mode

At the prompt, type the password. Note that it is case sensitive appears as stars (hidden).

You can type exit or Ctrl-z to exit this mode.

NOTE

The # prompt shows that you are in Privileged Mode.

The following example shows how to access Privileged mode as a guest user:

```
login as: guest
guest@172.30.106.124's password: voltaire
...
4036-006E> enable
password: ****** [123456]
Type Ctrl-z to exit from enable mode to disable mode.
4036-006E#
```

(Note that you have to login first in guest mode and then you can access the Privileged mode)

The following example shows how to access **directly** the Privileged mode as an admin user:

```
login as: admin
admin@172.30.106.124's password: ******    [123456]
...
4036-006E #
```

18.3 Admin (Privileged) Mode Command Reference

The commands available in **Admin** mode and their descriptions are listed below.

```
4036-006E# ?
<command> ?             Displays the command usage string
?                       Displays the list of available commands
cable-config show       Shows the cable configuration
clock show              Shows the system clock
config                  Changes to Configuration mode
debug                   Change to debug mode
disable                 Changes to Guest mode
end                     Ends the CLI
exit                    Exits to previous menu
firmware-version show   Show firmware version information
front show              Shows the blade module information at the front of
                        the chassis
health-monitor          Changes to Health Monitor mode
info-led set            Sets the info LED state
info-led show           Shows the info LED state
logs                    Changes to display logs menu
password update         Changes the admin or the enable password
ping                    Sends ping messages
reload                  Restarts the switch software
remote show             Shows the remote client configuration
route default-gw show   Shows the default gateway IP address
sm-info show            Shows the Subnet Manager (SM) parameters
temperature show        Shows the board temperature in Celsius and
                        Fahrenheit
Update firmware chassis Updates the firmware
                        version (embedded in the software update) using
                        previously defined server name, user name, and
                        password.
update software         Updates the software version using previously
                        defined server name, user name, and password
utilities               Changes to switch debug Utilities mode
version show            Shows software version information
```

Syntax usage is as follows in 4036/2036 **Admin** menu:

```
cable-config show                cable-config show
clock show                       clock show
config                           config
debug                            debug
disable                          disable
firmware-version show            firmware-version show
front show                       front show
health-monitor                   health-monitor
info-led set                     info-led set [off, blink]
info-led show                    Shows the info LED state
logs                             logs
password update                  password update [admin, enable, guest,
                                 root]
ping                             ping [ip-address]
reload                           reload
remote show                      remote show
route default-gw show            default-gw show
sm-info show                     sm-info show
temperature show                 Shows the board temperature in Celsius and
                                 Fahrenheit
update firmware chassis          update firmware chassis [update-file-dir
                                 (if not present, takes local)]
update software                  update software [update-file-dir]
utilities                        utilities
version show                     version show
```

The following details the commands available in Privileged mode:

---

cable-config show

Description: Shows the cable configuration. The system is able to automatically detect cable information if it is available.

Values: Cable is not present – no cable in installed in this port.

Cable is present – a cable is installed in this port but no cable information is available.

Cable information – a cable is installed in this port and the cable information is detailed.

Cable error – error reading the cable information.

Supported cables – Contact Voltaire Technical Support.

Syntax: `cable-config show`

Example:

```
4036-006E> cable-config show
Port#  1: Not present
Port#  2: Not present
Port#  3: Not present
```

```
Port#  4: Not present
Port#  5: Not present
Port#  6: Not present
Port#  7: Not present
Port#  8: Not present
Port#  9: Not present
Port# 10: Not present
Port# 11: Not present
Port# 12: Not present
Port# 13: Not present
Port# 14: Not present
Port# 15: Not present
Port# 16: Not present
Port# 17: Not present
Port# 18: Not present
Port# 19: Not present
Port# 20: Not present
Port# 21: Not present
Port# 22: length 1 Vendor Name: WLGORE Code: QSFP Vendor PN: SCN-2012-9
Vendor Rev: P1 Vendor SN: 070108-060
Port# 23: Not present
Port# 24: Not present
Port# 25: Not present
Port# 26: Not present
Port# 27: Not present
Port# 28: Not present
Port# 29: Not present
Port# 30: Not present
Port# 31: Not present
Port# 32: Not present
Port# 33: Not present
Port# 34: length 1 Vendor Name: WLGORE Code: QSFP Vendor PN: SCN-2012-9
Vendor Rev: P1 Vendor SN: 070108-060
Port# 35: Not present
Port# 36: Not present
```

clock show

Description: Displays the time and date currently set in the switch.

Syntax: `clock show`

Example:

```
4036-006E# clock show
Mon Feb 16 01:22:16 UTC 2009
```

config

Description: Changes to the Configuration mode, which allows the user to configure the 4036/2036 advanced parameters. Configuration (config) Mode is

detailed in 0.

Syntax: `config`

debug

Description: Changes to Debug mode, which is intended for the use of Voltaire personnel only.

Syntax: `debug`

disable

Description: Disables the **Admin** mode and switches to the **Guest** mode, which allows view-only access of the switch configuration parameters.

Syntax: `disable`

firmware-version show

Description: Shows the firmware version information as well as the PSID indicator. The PSID is an indicator associated with each firmware image to allow firmware identification. This command is used to list the firmware version and the PSID indicator for all the switch chips in the fabric. The following is and example of PSID format: VLT1150031011.

Syntax: `firmware-version show`

Example:

```
4036-006E# firmware-version show
FW Version:         7.1.948
PSID:               VLT1220030706
```

front show

Description: Shows the blade module information as it appears at the front of the chassis.

Syntax: `front show`

Example:

```
036-0076# front show
Device:2036 Temperature: 45C normal
HW Version   : A02
Serial Number: AL4608000120
PS #1: ok
PS #2: ok
```

```
Num of fans: 6
Fans rate: normal
Fans direction: IN fault
Fan #1: ok
Fan #2: ok
Fan #3: ok
Fan #4: ok
Fan #5: ok
Fan #6: ok
The system DC power consumption is 38 W
```

Health Monitor

Description: Changes to the Health Monitor Mode. The Health Monitor Menu is detailed in section 18.4, "Health Monitor"

Syntax: `Health Monitor`

info-led set

Description: Sets the info LED state

Syntax: `info-led set [off, blink]`

Default: off

Example: `info-led set blink`

info-led show

Description: Shows the info LED state

Syntax: `info-led show`

Example:

```
4036-006E# info-led show
Info LED is blink
```

logs

Description: Changes to the Logs Mode. The Logs Menu is detailed in section 18.5.

Syntax: `logs`

password update

Description: Changes the password.

Syntax: `password update [admin,enable,guest,root]`

Note that you can update the root password from here.

Default: Default passwords are as follows:

guest: `voltaire`

admin: `123456`

root: Please contact your Support representative.

Example: password update `[admin,enable,guest,root]`

1. Type password update **root**. You are prompted to insert a new (8 characters) password.
2. Type in the new password.
3. When prompted again, make sure you retype the password exactly as was done in the previous step. You have now changed the root password in the CLI.

---

ping

Description: Sends ping messages to network hosts. Pings a specified network host up to four times**.** Press Ctrl-C to stop pinging.

Syntax: `ping`

Example:

```
4036-006E# ping 172.30.106.30
PING 172.30.106.30 (172.30.106.30): 56 data bytes
64 bytes from 172.30.106.30: icmp_seq=0 ttl=64 time=0.2 ms
64 bytes from 172.30.106.30: icmp_seq=1 ttl=64 time=0.1 ms
64 bytes from 172.30.106.30: icmp_seq=2 ttl=64 time=0.1 ms
64 bytes from 172.30.106.30: icmp_seq=3 ttl=64 time=0.1 ms

--- 172.30.106.30 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
```

---

reload

Description: Reboots the switch; this command is required after performing various software operations in order for configuration changes to take effect. This is a software reset.

Syntax: `reload`

remote show

Description: Shows the remote client configuration.

Default: There is no default remote client. You must define it if required.

Syntax: `remote show`

Example:

```
4036-006E# remote show
remote configuration
----------------------
remote server: 172.25.5.48
username:      root
protocol:      SCP
```

route default-gw show

Description: Shows the default gateway IP address.

Syntax: `route default-gw show`

Default: There is no default gateway. You must define it if required.

Example:

```
4036-006E# route default-gw show
default-gw is: 172.28.0.1
```

sm-info show

Description: Shows the Subnet Manager (SM) parameters.

Syntax: `sm-info show`

Default:

```
4036-006E# sm-info show
subnet manager info is:
sm routing_engine = minhop
sm sweep_interval = 15
sm max_wire_smps = 16
sm priority = 4
sm LMC = 0
sm max_op_vls = 5
sm transaction_timeout = 150
sm head_of_queue_lifetime = 0x10
sm leaf_head_of_queue_lifetime = 0x10
sm packet_life_time = 0x12
sm sminfo_polling_timeout = 5000
sm polling_retry_number = 12
sm reassign_lids = disable
```

```
sm babbling_port_policy = disable
sm state = standby
sm mode = enable
```

Example:

```
4036-006E# sm-info show
subnet manager info is:
sm routing_engine = minhop
sm sweep_interval = 20
sm max_wire_smps = 5
sm priority = 10
sm LMC = 6
sm max_op_vls = 5
sm transaction_timeout = 240
sm head_of_queue_lifetime = 10
sm leaf_head_of_queue_lifetime = 10
sm packet_life_time = 10
sm sminfo_polling_timeout = 1100
sm polling_retry_number = 100
sm reassign_lids = disable
sm babbling_port_policy = disable
sm state = standby
sm mode = enable
```

temperature show

Description: Shows the board temperature in Celsius and in Fahrenheit

Syntax: `temperature show`

Default: Temperature threshold:

Warning = 60

Alarm = 80

Relax (normal) =40

Example:

```
4036-006E# temperature show
Temperature sensor #0[alarm (T>=30)]: 41[C], 105[F]
Temperature sensor #1[alarm (T>=30)]: 41[C], 105[F]
Temperature sensor #2[alarm (T>=30)]: 41[C], 105[F]
Temperature sensor #3[alarm (T>=30)]: 42[C], 107[F]
```

update firmware chassis

Description: Updates the firmware version (Embedded in the software update) using previously defined server name, user name, and password.

Syntax: `update firmware chassis [update-file-dir (if not present, takes local)]`

Default: Local path (see syntax)

Example:

```
4036-006E# update firmware chassis

-W- Unknown device id (23130) in the given FW image. Skipping HW match check.


    Current FW version on flash:  7.1.938
    New FW version:               7.1.938


    Note: The new FW version is not newer than the current FW version on flash.


 Do you want to continue ? (y/n) [n] : y

Burning second FW image without signatures  - OK
Restoring second signature                  - OK
```

update software

Description: Updates the software version using the previously defined server name, user name, and password. (Sets remote server information from the Remote submenu under Configuration mode)

Syntax: `update software [update-file-dir]`

Example:

```
4036-006E#  update software /pub/versions/install
```

utilities

Description: changes to Utilities Mode. The Utilities Menu is detailed in section 18.6, "Utilities Mode".

Syntax: `utilities`

version show

Description: Displays the software version information

Syntax: `version show`

Example:

```
4036-006E# version show
ISR 2036/4036 version: 2.0.0
        date:    Feb 15 2009 08:39:54 AM
```

```
        build Id:1000
```

18.4 Health Monitor

The Health Monitor menu provides the list of buil-in-tests that are available for this system.

This menu provides the commands available in Health Monitor Mode.

```
4036-006E# health-monitor
4036-006E(hm)# ?
<command> ?     Displays the command usage string
?               Displays the list of available commands
bit             Executes tests as part of built in test procedure.
                Execute all the tests by typing all. Executes one or
                several tests by typing the test identifiers separated by
                comma (for example: 2,5,6)
bit-show        Shows all available built in tests with identifier and
                description
end             Ends the CLI
exit            Exits to previous menu
```

Health Monitor syntax usage is as follows:

```
bit                         bit [test identifier, list of tests, all]
bit-show                    bit-show
```

The following details the commands available under the Health Monitor Menu.

---

bit

Description: Executes tests as part of the Built-in-Test procedure.

When logging in Admin mode, the Built in Test runs several tests before entering the CLI session. This feature provides the ability to run any script was pre-defined by the CLI interface. You can also run this test manually from the Health Monitor sub menu. Note that this test runs automatically when logging into the CLI.

Execute all the tests by typing all.
Execute one or several tests by typing the test identifiers separated by a comma (for example: 2,5,6).

Syntax: `bit`

Example:

```
4036-006E(hm)# bit 2
Checking the fan direction ...                  done
```

bit-show

Description: Shows all available built-in-tests with identifiers and descriptions.

Syntax: `bit-show`

Example:

```
4036-006E(hm)# bit-show
-------------------------------------------------
BIT Identifier      Description
-------------------------------------------------
1                   bit_proc_tight_loop_check.sh
2                   bit_fan_direction_check
```

18.5 Logs Mode

This menu shows the logs menu and utilities enhancing current diagnostic features and adding diagnostic functionality. This is for remote support activities. When experiencing a problem with your system, support might request to provide them some of the following logs.

Note that if logs are long, press **Enter** on your keyboard to view more.
Click **Ctrl + C** to exit.

This menu provides the commands available in Logs Mode.

```
4036-006E(logs)# ?
<command> ?             Displays the command usage string
?                       Displays the list of available commands
cli-log show            Shows the CLI log file
end                     Ends the CLI
error-log show          Shows the switch error log
event-log show          Shows the switch event log
exit                    Exits to previous menu
remote-logger delete    Deletes the remote-logger (syslog) of this switch
remote-logger set       Set the remote-logger (syslog) of this switch.
remote-logger show      Shows the remote-logger (syslog) of this switch
sm-log show             Shows the SM log file
umServer-log show       Shows the umServer log file
```

Logs syntax usage is as follows:

```
cli-log show            cli-log show
error-log show          error-log show
event-log show          event-log show
remote-logger delete    remote-logger delete
remote-logger set       remote-logger set [ip]
remote-logger show      remote-logger show
sm-log show             Shows the SM log file
umServer-log show       Shows the umServer log file
```

The following details the commands available under the Logs Menu.

cli-log show

Description: Shows the CLI log file. Shows all the CLI logs that the user entered.

Syntax: `cli-log show`

Example:

```
4036-006E(logs)# cli-log show
Apr 24 12:40:42 voltaire4036 cli[428]: 152 general.cpp#436: COMMAND: config
Apr 24 12:40:45 voltaire4036 cli[428]: 152 general.cpp#436: COMMAND:
interface
Apr 24 12:40:46 voltaire4036 cli[428]: 152 general.cpp#436: COMMAND: ?
Apr 24 12:40:49 voltaire4036 cli[428]: 152 ipFuncsSw.cpp#545: fast
interface ip 192.168.1.2
Apr 24 12:40:49 voltaire4036 cli[428]: 152 general.cpp#436: COMMAND: ip-
address show
Apr 24 12:41:03 voltaire4036 cli[428]: 152 ipFuncsSw.cpp#273: Executing
command: sudo /sbin/ifconfig eth0 172.30.106.124.
Apr 24 12:41:03 voltaire4036 cli[428]: 152 localATS.cpp#44: IN
...
```

error-log show

Description: Shows the error log file. Error Log messages can be as follows:

```
WARNING, Temperature exceeded the warning threshold
CRITICAL, Temperature exceeded the alarm threshold
CRITICAL, Fan Unit was extracted
CRITICAL, could not perform fan direction validation
CRITICAL, Fan air flow direction does not match the system type
WARNING, Fan #1 fault
CRITICAL, All fans in the Fan Unit have failed
WARNING, Some fans in the Fan Unit have failed
WARNING, Fans rate in turbo mode
CRITICAL, PS #1: power failure
CRITICAL, PS #1: not present
CRITICAL, monitor execution failed
CRITICAL, Could not perform fan air flow direction validation
```

Syntax: `error-log show`

Example:

```
4036-006E(logs)# error-log show
Apr 24 15:25:02 voltaire4036 Update_software: "Succeeded."
Apr 25 16:12:45 voltaire4036 Update_software: "Succeeded."
Apr 28 11:18:23 voltaire4036 Update_software: "Succeeded."
```

```
Apr 28 17:12:36 voltaire4036 umServer[728]: trap state is now WARNING!
Apr 28 17:13:26 voltaire4036 umServer[754]: trap state is now WARNING!
Apr 28 17:42:04 voltaire4036 umServer[884]: trap state is now ALARM!
```

event-log show

Description: Shows the event log file. Event Log messages can be as follows:

```
NORMAL, Temperature is within the normal range
NORMAL, Fan Unit was inserted
NORMAL, Fan air flow direction matches system type
NORMAL, Fan #1 is now O.K
WARNING, NOT all fans are now in fault state
NORMAL, All fans in the Fan Unit are operational
NORMAL, Fans rate in normal mode
NORMAL, PS #1: power is O.K
SM state changed to NOT ACTIVE
SM state changed to DISCOVER
SM state changed to STANDBY
SM state changed to MASTER
NORMAL, Fan air flow direction matches system type
```

Syntax: `event-log show`

Example:

```
4036-006E(logs)# event-log show
Apr 24 15:25:02 voltaire4036 Update_software: "Succeeded."
Apr 25 16:12:45 voltaire4036 Update_software: "Succeeded."
Apr 28 11:18:23 voltaire4036 Update_software: "Succeeded."
Apr 28 11:21:53 voltaire4036 umServer[356]: PS #2 is now DC FAULT!
Apr 28 11:21:53 voltaire4036 umServer[356]: SM state changed to NOT ACTIVE
Apr 28 12:33:08 voltaire4036 umServer[286]: PS #2 is now DC FAULT!
Apr 28 12:33:09 voltaire4036 umServer[286]: SM state changed to NOT ACTIVE
Apr 28 14:57:38 voltaire4036 umServer[262]: PS #2 is now DC FAULT!
Apr 28 14:57:38 voltaire4036 umServer[262]: SM state changed to NOT ACTIVE
Apr 28 14:57:48 voltaire4036 umServer[262]: SM state changed to NOT ACTIVE
Apr 28 16:10:58 voltaire4036 umServer[557]: PS #2 is now DC FAULT!
Apr 28 16:23:51 voltaire4036 umServer[599]: PS #2 is now DC FAULT!
Apr 28 16:25:31 voltaire4036 umServer[628]: PS #2 is now DC FAULT!
Apr 28 17:11:25 voltaire4036 umServer[702]: PS #2 is now DC FAULT!
Apr 28 17:12:36 voltaire4036 umServer[728]: trap state is now WARNING!
Apr 28 17:12:37 voltaire4036 umServer[728]: PS #2 is now DC FAULT!
Apr 28 17:13:26 voltaire4036 umServer[754]: trap state is now WARNING!
Apr 28 17:13:26 voltaire4036 umServer[754]: PS #2 is now DC FAULT!
Apr 28 17:26:08 voltaire4036 umServer[816]: PS #2 is now DC FAULT!
Apr 28 17:41:14 voltaire4036 umServer[858]: PS #2 is now DC FAULT!
Apr 28 17:42:04 voltaire4036 umServer[884]: trap state is now ALARM!
Apr 28 17:42:05 voltaire4036 umServer[884]: PS #2 is now DC FAULT!
```

remote-logger delete

Description: Deletes the switch remote-logger IP address (syslog). Logs may be stored on a specific machine. In order to do this, this machine IP address needs to be configured on the switch. This command allows you to remove the machine IP address defined on the switch.

Syntax: `remote-logger delete`

Example:

```
4036-006E(logs)# remote-logger delete
```

remote-logger set

Description: Sets the switch remote-logger IP address (syslog). Logs may be stored on a specific machine. In order to do this, this machine IP address needs to be configured on the switch. This command allows you to define the machine IP address on the switch.

Syntax: `remote-logger set [ip]`

Default: There is no default remote logger. You must define it if required.

Example:

```
4036-006E(logs)# remote-logger set 172.25.2.206
```

remote-logger show

Description: Shows the switch remote-logger IP address (syslog). Logs may be stored on a specific machine. In order to do this, this machine IP address needs to be configured on the switch. This command allows you to view the machine IP address defined on the switch.

Syntax: `remote-logger show`

Example:

```
4036-006E(logs) remote-logger show
remote logger is 172.25.2.206
```

sm-log show

Description: Shows the Subnet Manager (SM) log, listing the events according to the user configuration of verbosity.

Syntax: `sm-log show`

Example:

```
4036-006E(logs)# sm-log show
```

```
4 -> si_rcv_process_existing: discovery_count is:1
Apr 07 12:05:02 630213 [4905D4B0] 0x04 -> si_rcv_process_existing:
discovery_count is:1
Apr 07 12:05:02 630501 [4905D4B0] 0x04 -> si_rcv_process_existing:
discovery_count is:1
Apr 07 12:05:02 630815 [4905D4B0] 0x04 -> si_rcv_process_existing:
discovery_count is:1
Apr 07 12:05:02 631068 [4905D4B0] 0x04 -> si_rcv_process_existing:
discovery_count is:2
...
```

umServer-log show

Description: Shows the umServer log file. This log is used if you have a problem with the internal management server.

Syntax: `umServer-log show`

Example:

```
Switch(logs) umServer-log show
Apr  7 17:50:04 0 umServer[832]: getFromRepository#39: IN
Apr  7 17:50:05 0 umServer[832]: getFromRepository#52: OUT
Apr  7 17:50:05 0 umServer[832]: Starting umServer
```

18.6 Utilities Mode

This menu provides advanced scripts and utilities enhancing current diagnostic features and adding diagnostic functionality.

```
<command> ?     Displays the command usage string
?               Displays the list of available commands
end             Ends the CLI
exit            Exits to previous menu
ibaddr          Shows the lid and GID addresses of the specified port.
ibchecknet      Scans the network to validate the connectivity.
ibcheckwidth    Scans the network to validate the active link widths.
ibclearcounters Clears the PMA port counters
ibclearerrors   Clears the PMA error counters in PortCounters
ibhosts         Extracts the CA nodes.
ibnetdiscover   Performs  IB subnet discovery
ibportstate     Queries the port state and port physical state of an IB
                port.
ibswitches      Extracts the IB switches.
ibtracert       Traces the path from a source GID/LID to a destination
                GID/LID.
perfquery       Obtains the PortCounters (basic performance and error
                counters) from the PMA at the node specified.
port verify     Performs a port-verify command
sminfo          Queries information from the operational Subnet Manager
               (SM).
smpquery        Allows a basic subset of standard SMP queries.
vendstat        Queries vendor-specific information of a switch LID.
```

Utilities syntax usage:

```
ibaddr          ibaddr [options] [<lid|dr_path|guid>]

ibchecknet      bchecknet [-h] [-v] [-N | -nocolor] [<topology-file> |
                -C ca_name -P ca_port -t(imeout) timeout_ms]

ibcheckwidth    ibcheckwidth [-h] [-v] [-N | -nocolor]
                [<topology-file> \| -C ca_name -P ca_port -t(imeout)
                timeout_ms]

ibclearcounters [-h] [<topology-file> | -C ca_name -P ca_port -t(imeout)
                timeout_ms]

ibclearerrors  [-h] [-N | -nocolor] [<topology-file> | -C ca_name
                -P ca_port  -t(imeout) timeout_ms]

ibhosts         ibhosts [-h] [<topology-file> | -C ca_name -P ca_port
                -t(imeout) timeout_ms]

ibnetdiscover   ibnetdiscover [options] [topology-file]

                -p(orts) [<topology-file>]
```

```
ibportstate     ibportstate [options] <dest dr_path|lid|guid> <portnum>
                [<op>]

                Supported ops: enable, disable, reset, speed, query

ibswitches      ibswitches [-h] [<topology-file> | -C ca_name
                -P ca_port -t(imeout) timeout_ms]

ibtracert       ibtracert [options] <src-addr> <dest-addr>

perfquery       perfquery [options]  [<lid|guid> [[port] [reset_mask]]]

port-verify     port-verify –h
                port-verify [options] [topology-file]

smpquery        smpquery [options] <op> <dest dr_path|lid|guid> [op params]

                Supported ops (and aliases, case insensitive):
                NodeInfo (NI) <addr>
                NodeDesc (ND) <addr>
                PortInfo (PI) <addr> [<portnum>]
                SwitchInfo (SI) <addr>
                PKeyTable (PKeys) <addr> [<portnum>]
                SL2VLTable (SL2VL) <addr> [<portnum>]
                VLArbitration (VLArb) <addr> [<portnum>]
                GUIDInfo (GI) <addr>

vendstat        vendstat [options] <lid|guid>
```

The following details the common options available in the Utilities commands.

Common Options

The supported options are listed in each utility. You can use the –h option to get more information on each utility and the various options.

Table 18-1. Common Options

Option	Description
Debugging options	
-d	Raises the InfiniBand debugging level. May be used several times (-ddd or -d -d -d)
-e	Shows the send and receive errors (timeouts and others)
-h	Shows the help.

Option	Description
-v	Increases the application verbosity level. May be used several times (-vv or -v - -v)
-V	shows the version information.
Addressing Options	
-D	Use the direct path address arguments. The path is a comma separated list of out ports. Examples: "0" # self port "0,1,2,1,4" # out via port 1, then 2, ...
-G	Use the GUID address argument. In most cases, it is the Port GUID. Example: "0x08f1040023"
-s <smlid>	Use 'smlid' as the target lid for SM/SA queries.
Additional Common Options	
-h	Provides help
-v	Increases the application verbosity level. May be used several times (-vv or -v -v -v)
-N/-nocolor	The output of the command is displayed in one color (default color on your terminal).
Topology file	Runs the command on a simulation file.
-C ca_name (*)	Channel adapter name (ca_name). Currently, the default for the 4036/2036 switches is: is4_0.
-P ca_port (*)	Channel adapter port number (ca_port). Currently, the default for the 4036/2036 switches is: 0.
-t(timout) timeout_ms	Timeout for answers. Overrides the default timeout for the solicited mads.

(*) Using options –C and –P

These options inform utilities which channel adapter (C) and which port (P) to use in order to reach a specific InfiniBand fabric based on the specific selection.

By default, the 4036/2036 switch channel adapter is is4_0 the port (0). Therefore, not specifying –C and –P will implement the default.

The following details the commands available under the Utilities Menu.

---

ibaddr

Description: `ibaddr` queries InfiniBand addresses. It can be used to show the LID and GID addresses of the specified port or the local port by default.

Note: this utility can be used as simple address resolver.

Syntax:

```
4036-006E(utilities)# ibaddr --help
ibaddr [options] [<lid|dr_path|guid>]
```

Options:

```
  --gid_show, -g          show gid address only
  --lid_show, -l          show lid range only
  --Lid_show, -L          show lid range (in decimal) only
  --Ca, -C <ca>           Ca name to use
  --Port, -P <port>       Ca port number to use
  --Direct, -D            use Direct address argument
  --Guid, -G              use GUID address argument
  --timeout, -t <ms>      timeout in ms
  --sm_port, -s <lid>     SM port lid
  --errors, -e            show send and receive errors
  --verbose, -v           increase verbosity level
  --debug, -d             raise debug level
  --usage, -u             usage message
  --help, -h              help message
  --version, -V           show version
```

Dependencies: ibroute, ibtracert

Examples:

```
  ibaddr                # local port's address
  ibaddr 32             # show lid range and gid of lid 32
  ibaddr -G 0x8f1040023 # same but using guid address
  ibaddr -l 32          # show lid range only
  ibaddr -L 32          # show decimal lid range only
  ibaddr -g 32          # show gid address only
```

ibchecknet

Description: ibchecknet is a script which uses a full topology file that was created by ibnetdiscover, and scans the network to validate the connectivity and reports errors (from port counters).

Syntax:

```
4036-006E(utilities)# ibchecknet --help
Usage: ibchecknet [-h] [-v] [-N | -nocolor] [<topology-file> | -C ca name -
P ca_port -t(imeout) timeout_ms]
```

Dependencies: ibnetdiscover, ibnetdiscover format, ibchecknode, ibcheckport, ibcheckerrs

Example:

```
4036-006E(utilities)# ibchecknet
#warn: counter SymbolErrors = 65531     (threshold 10) lid 8 port 255
#warn: counter LinkRecovers = 206       (threshold 10) lid 8 port 255
#warn: counter RcvErrors = 43           (threshold 10) lid 8 port 255
#warn: counter RcvSwRelayErrors = 11886 (threshold 100) lid 8 port 255
#warn: counter XmtDiscards = 361        (threshold 100) lid 8 port 255
#warn: counter LinkIntegrityErrors = 15 (threshold 10) lid 8 port 255
Error check on lid 8 (Voltaire 4036 - 36 QDR ports switch) port all:
FAILED
#warn: counter LinkRecovers = 10        (threshold 10) lid 8 port 30
Error check on lid 8 (Voltaire 4036 - 36 QDR ports switch) port 30:  FAILED
#warn: counter LinkRecovers = 10        (threshold 10) lid 8 port 29
Error check on lid 8 (Voltaire 4036 - 36 QDR ports switch) port 29:  FAILED
#warn: counter SymbolErrors = 65535     (threshold 10) lid 10 port 255
#warn: counter LinkDowned = 68          (threshold 10) lid 10 port 255
#warn: counter RcvSwRelayErrors = 65535 (threshold 100) lid 10 port 255
#warn: counter XmtDiscards = 25009      (threshold 100) lid 10 port 255
#warn: counter VL15Dropped = 65535      (threshold 100) lid 10 port 255
Error check on lid 10 (ISR9288/ISR9096 Voltaire sLB-24D) port all:  FAILED
#warn: counter VL15Dropped = 245        (threshold 100) lid 10 port 12
…
```

ibcheckwidth

Description: Scans the network to validate the active link widths. `ibcheckwidth` uses a full topology file created by `ibnetdiscover`; it scans the network to validate the active link widths and reports any 1x links.

Syntax:

```
4036-006E(utilities)# ibcheckwidth -h
Usage: ibcheckwidth [-h] [-v] [-N | -nocolor] [<topology-file> \| -C
ca_name -P ca_port -t(imeout) timeout_ms]
```

Options are detailed in Table 18-1.

Dependencies: `ibnetdiscover, ibnetdiscover format, ibchecknode, ibcheckportwidth`

Example:

```
4036-006E(utilities)# ibcheckwidth

## Summary: 17 nodes checked, 0 bad nodes found
##          210 ports checked, 0 ports with 1x width in error found
```

ibclearcounters

Description: Clears the **Performance Manager Agent** (PMA) port counters.

Note: PMA – Performance Manager Agent

PMA port counters and errors can be viewed by running a perfquery command, as shown below.

```
# perfquery
# Port counters: Lid 1 port 0
PortSelect:......................0
CounterSelect:...................0x1b01
```

PMA counters

```
SymbolErrors:....................0
LinkRecovers:....................0
LinkDowned:......................0
RcvErrors:.......................0
RcvRemotePhysErrors:.............0
RcvSwRelayErrors:................10661
XmtDiscards:.....................0
XmtConstraintErrors:.............0
RcvConstraintErrors:.............0
CounterSelect2:..................0
LinkIntegrityErrors:.............0
ExcBufOverrunErrors:.............0
```

PMA errors

```
VL15Dropped:.....................0
XmtData:.........................21600
RcvData:.........................999000
XmtPkts:.........................300
RcvPkts:.........................13875
XmtWait:.........................129
```

Syntax:

```
4036-006E(utilities)# ibclearcounters -h
Usage: ibclearcounters [-h] [<topology-file> | -C ca_name -P ca_port -
t(imeout) timeout_ms]
```

Options are detailed in Table 18-1.

Dependencies: `ibnetdiscover, perfquery`

Example:

```
Ibclearcounters –C <ca_name> –P<ca_port>
```

This clears all the counters for this chassis in the fabric.

---

ibclearerrors

Description: `ibclearerrors` clears the PMA error counters in PortCounters by either walking the InfiniBand subnet topology or using an already saved topology file.

Note: PMA – Performance Manager Agent

PMA port counters and errors can be viewed by running a perfquery command, as shown below.

```
# perfquery
# Port counters: Lid 1 port 0
PortSelect:......................0
CounterSelect:...................0x1b01
...
```

PMA errors

```
VL15Dropped:.....................0
XmtData:.........................21600
RcvData:.........................999000
XmtPkts:.........................300
RcvPkts:.........................13875
XmtWait:.........................129
```

Syntax:

```
4036-006E(utilities)# ibclearerrors -h
Usage: ibclearerrors [-h] [-N | -nocolor] [<topology-file> | -C ca_name -P
ca_port -t(imeout) timeout_ms]
```

Options are detailed in Table 18-1.

Dependencies: `ibnetdiscover, ibnetdiscover format`

Example:

```
Ibclearerrors -C <ca_name> -P<ca_port>
```

This clears all the errors for this chassis in the fabric.

ibhosts

Description: Discovers and lists the Channel Adapter nodes in the fabric.

Syntax:

```
4036-006E(utilities)# ibhosts --help
Usage: ibhosts [-h] [<topology-file> | -C ca_name -P ca_port -t(imeout)
timeout_ms]
```

Options are detailed in Table 18-1.

Dependencies: `ibnetdiscover`

Example:

```
4036-006E(utilities)# ibhosts
Ca      : 0x0008f1040399f464 ports 2 " HCA-1"
```

ibnetdiscover

Description: Discovers and lists the Switches, routers, and CA nodes in the fabric by Performing an InfiniBand subnet discovery and outputting a readable topology file. GUIDs, node types, and port numbers are displayed as well as port LIDs and node descriptions. All nodes and links are displayed (full topology). Optionally this utility can be used to list the nodes currently connected. The output is printed to the standard output unless a topology file is specified.

Syntax:

```
4036-0076(utilities)# ibnetdiscover --help
Usage: ibnetdiscover [options] [topology-file]
```

Options:

```
  --show, -s              shows more information
  --list, -l              provides a list of connected nodes
  --grouping, -g          shows grouping
  --Hca_list, -H          provides a list of connected CAs
  --Switch_list, -S       provides a list of connected switches
  --Router_list, -R       provides a list of connected routers
  --node-name-map <file>  node name map file. The node name map file maps
                          GUIDs  to more user-friendly names.
  --ports, -p             obtains a port report, which is a list of
                          connected ports with relevant information
                          like LID, portnum,  GUID,  width,  speed, and
                          Node Description).
```

```
--Ca, -C <ca>           Ca name to use
--Port, -P <port>       Ca port number to use
--timeout, -t <ms>      timeout in ms
--errors, -e            shows send and receive errors
--verbose, -v           increases verbosity level
--debug, -d             raises debug level
--usage, -u             usage message
--help, -h              help message
--version, -V           shows the version
```

Options are detailed in Table 18-1.

TOPOLOGY FILE FORMAT

The topology file format is human readable and largely intuitive. Most identifiers are given textual names like vendor ID (vendid), device ID (device ID), GUIDs of various types (sysimgguid, caguid, switchguid, etc.). PortGUIDs are shown in parentheses (). For switches, this is shown on the switchguid line. For CA and router ports, it is shown on the connectivity lines. The IB node is identified followed by the number of ports and a quoted the node GUID. On the right of this line is a comment (#) followed by the Node Description in quotes. If the node is a switch, this line also contains whether switch port 0 is base or enhanced, and the LID and LMC of port 0. Subsequent lines pertaining to this node show the connectivity.

On the left is the port number of the current node. On the right is the peer node (node at other end of link). It is identified in quotes with nodetype followed by - followed by NodeGUID with the port number in square brackets. Further on the right is a comment (#). What follows the comment is dependent on the node type. If it is a switch node, it is followed by the NodeDescription in quotes and the LID of the peer node. If it is a CA or router node, it is followed by the local LID and LMC and then followed by the NodeDescription in quotes and the LID of the peer node. The active link width and speed are then appended to the end of this output line.

When grouping is used, InfiniBand nodes are organized into multiple chassis which are numbered. Nodes which cannot be determined to be in a chassis are displayed as "Non-Chassis Nodes". External ports are also shown on the connectivity lines.

NODE NAME MAP FILE FORMAT

The node name map is used to specify user friendly names for nodes in the output. GUIDs are used to perform the search.

Generic:

<guid> "<name>"

Example:

The following example shows all the switches in the fabric.

```
4036-006E(utilities)# ibnetdiscover -S
Switch   : 0x0008f1050010006e ports 36 devid 0x5a40 vendid 0x8f1 "Voltaire
4036 - 36 QDR ports switch"
Switch   : 0x0008f104003f2851 ports 24 devid 0x5a38 vendid 0x8f1
"ISR2012/ISR2004 Voltaire sLB-2024"
Switch   : 0x0008f100010c0052 ports 36 devid 0x5a09 vendid 0x8f1 "Voltaire
2036 - 36 DDR ports switch"
Switch   : 0x0008f100010c005c ports 36 devid 0x5a09 vendid 0x8f1 "Voltaire
2036 - 36 DDR ports switch"
Switch   : 0x0008f100010c0036 ports 36 devid 0x5a5a vendid 0x8f1 "Voltaire
4036 - 36 QDR ports switch"
Switch   : 0x0008f104004038f7 ports 24 devid 0x5a40 vendid 0x8f1 "ISR2004
Voltaire sFB-2004"
Switch   : 0x0008f104004038d3 ports 24 devid 0x5a40 vendid 0x8f1 "ISR2004
Voltaire sFB-2004"
Switch   : 0x0008f104004038ef ports 24 devid 0x5a40 vendid 0x8f1 "ISR2004
Voltaire sFB-2004"
Switch   : 0x0008f104004038fb ports 24 devid 0x5a40 vendid 0x8f1 "ISR2004
Voltaire sFB-2004"
Switch   : 0x0008f104003f2850 ports 24 devid 0x5a38 vendid 0x8f1
"ISR2012/ISR2004 Voltaire sLB-2024"
Switch   : 0x0008f104003f1df7 ports 24 devid 0x5a38 vendid 0x8f1
"ISR2012/ISR2004 Voltaire sLB-2024"
Switch   : 0x0008f104003f1df6 ports 24 devid 0x5a38 vendid 0x8f1
"ISR2012/ISR2004 Voltaire sLB-2024"
Switch   : 0x0008f104003f1e69 ports 24 devid 0x5a38 vendid 0x8f1
"ISR2012/ISR2004 Voltaire sLB-2024"
Switch   : 0x0008f104003f1e68 ports 24 devid 0x5a38 vendid 0x8f1
"ISR2012/ISR2004 Voltaire sLB-2024"
Switch   : 0x0008f104003f68e9 ports 24 devid 0x5a38 vendid 0x8f1
"ISR2012/ISR2004 Voltaire sLB-2024"
Switch   : 0x0008f104003f68e8 ports 24 devid 0x5a38 vendid 0x8f1
"ISR2012/ISR2004 Voltaire sLB-2024"
```

ibportstate

Description: Queries the port state and port physical state of an InfiniBand port (in addition to the link width and speed being validated relatively to the peer port when the port queried is a switch port), or a switch port to be disabled, enabled, or reset. It also allows the link speed enabled on any InfiniBand port to be adjusted.

Syntax:

```
4036-0076(utilities)# ibportstate --help

Usage: ibportstate [options] <dest dr_path|lid|guid> <portnum> [<op>]

Supported ops: enable, disable, reset, speed, query
```

op Port operations allowed

Default is query

ops enable, disable, and reset are only allowed on switch ports (An error is indicated if attempted on CA or router ports) speed op is allowed on any port speed values are legal values for PortInfo:LinkSpeedEnabled (An error is indicated if PortInfo:LinkSpeedSupported does not support these settings)

NOTE: Speed changes are not effected until the port goes through link renegotiation)

Query also validates port characteristics (link width and speed) based on the peer port. This check is done when the port queried is a switch port as it relies on combined routing (an initial LID route with directed routing to the peer) which can only be done on a switch. This peer port validation feature of query op requires LID routing to be functioning in the subnet.

Options:

```
--Ca, -C <ca>           Ca name to use
--Port, -P <port>       Ca port number to use
--Direct, -D            use Direct address argument
--Lid, -L               use LID address argument
--Guid, -G              use GUID address argument
--timeout, -t <ms>      timeout in ms
--sm_port, -s <lid>     SM port lid
--errors, -e            show send and receive errors
--verbose, -v           increase verbosity level
--debug, -d             raise debug level
--usage, -u             usage message
--help, -h              help message
--version, -V           show version
```

Options are detailed in Table 18-1.

Examples:

```
ibportstate 3 1 disable                      # by lid
ibportstate -G 0x2C9000100D051 1 enable      # by guid
ibportstate -D 0 1                           # (query) by direct route
ibportstate 3 1 reset                        # by lid
ibportstate 3 1 speed 1                      # by lid
```

ibswitches

Description: Discovers the InfiniBand switches in the fabric.

Syntax:

```
4036-006E(utilities)# ibswitches --help
Usage: ibswitches [-h] [<topology-file> | -C ca_name -P ca_port -t(imeout)
timeout_ms]
```

Dependencies: `ibnetdiscover, ibnetdiscover format`

Example:

```
4036-006E(utilities)# ibswitches
Switch  : 0x0008f1050010006e ports 36 "Voltaire 4036 - 36 QDR ports switch"
enhanced port 0 lid 17 lmc 0
Switch  : 0x0008f104003f2851 ports 24 "ISR2012/ISR2004 Voltaire sLB-2024"
base port 0 lid 9 lmc 0
Switch  : 0x0008f100010c0052 ports 36 "Voltaire 2036 - 36 DDR ports switch"
enhanced port 0 lid 3 lmc 0
Switch  : 0x0008f100010c005c ports 36 "Voltaire 2036 - 36 DDR ports switch"
enhanced port 0 lid 1 lmc 0
Switch  : 0x0008f100010c0036 ports 36 "Voltaire 4036 - 36 QDR ports switch"
enhanced port 0 lid 2 lmc 0
Switch  : 0x0008f104004038f7 ports 24 "ISR2004 Voltaire sFB-2004" enhanced
port 0 lid 14 lmc 0
Switch  : 0x0008f104004038d3 ports 24 "ISR2004 Voltaire sFB-2004" base port
0 lid 12 lmc 0
Switch  : 0x0008f104004038ef ports 24 "ISR2004 Voltaire sFB-2004" base port
0 lid 13 lmc 0
Switch  : 0x0008f104004038fb ports 24 "ISR2004 Voltaire sFB-2004" enhanced
port 0 lid 15 lmc 0
Switch  : 0x0008f104003f2850 ports 24 "ISR2012/ISR2004 Voltaire sLB-2024"
base port 0 lid 8 lmc 0
Switch  : 0x0008f104003f1df7 ports 24 "ISR2012/ISR2004 Voltaire sLB-2024"
base port 0 lid 5 lmc 0
Switch  : 0x0008f104003f1df6 ports 24 "ISR2012/ISR2004 Voltaire sLB-2024"
base port 0 lid 4 lmc 0
Switch  : 0x0008f104003f1e69 ports 24 "ISR2012/ISR2004 Voltaire sLB-2024"
base port 0 lid 7 lmc 0
Switch  : 0x0008f104003f1e68 ports 24 "ISR2012/ISR2004 Voltaire sLB-2024"
base port 0 lid 6 lmc 0
Switch  : 0x0008f104003f68e9 ports 24 "ISR2012/ISR2004 Voltaire sLB-2024"
base port 0 lid 11 lmc 0
Switch  : 0x0008f104003f68e8 ports 24 "ISR2012/ISR2004 Voltaire sLB-2024"
base port 0 lid 10 lmc 0
```

ibtracert

Description: Traces the path from a source GID/LID to a destination GID/LID. Each hop along the path is displayed until the destination is reached or a hop does not respond. By using the -m option, multicast path tracing can be performed between source and destination nodes.

Syntax:

```
4036-0076(utilities)# ibtracert --help

Usage:
ibtracert [options] <src-addr> <dest-addr>
```

Options:

```
  --force, -f            force
```

```
--no_info, -n           simple format
--mlid, -m <mlid>       multicast trace of the mlid
--node-name-map <file>  node name map file
--Ca, -C <ca>           Ca name to use
--Port, -P <port>       Ca port number to use
--Direct, -D            use Direct address argument
--Lid, -L               use LID address argument
--Guid, -G              use GUID address argument
--timeout, -t <ms>      timeout in ms
--sm_port, -s <lid>     SM port lid
--errors, -e            show send and receive errors
--verbose, -v           increase verbosity level
--debug, -d             raise debug level
--usage, -u             usage message
--help, -h              help message
--version, -V           show version
```

Options are detailed in Table 18-1.

Dependencies: ibroute

Examples:

```
ibtracert - Unicast examples:
ibtracert 4 16                # show path between lids 4 and 16
ibtracert -n 4 16             # same, but using simple output format
ibtracert -G 0x8f1040396522d 0x002c9000100d051      # use guid addresses
ibtracert  - Multicast examples:
ibtracert -m 0xc000 4 16      # show multicast path of mlid 0xc000
                                between lids 4 and 16
```

Additional Example:

```
# ibtracert 2 4
From switch {0x0008f100010c005c} portnum 0 lid 2-2 "Voltaire 2036 - 36 DDR
ports switch"
[1] -> switch port {0x0008f1050010006e}[21] lid 4-4 "Voltaire 4036 - 36 QDR
ports switch"
To switch {0x0008f1050010006e} portnum 0 lid 4-4 "Voltaire 4036 - 36 QDR
ports switch"
```

perfquery

Description: Obtains the PortCounters (basic performance and error counters) from the PMA at the specified node.

`perfquery` uses PerfMgt GMPs to obtain the PortCounters (basic performance and error counters) from the PMA at the node specified. Optionally show aggregated counters for all ports of node. Also, optionally, reset after read, or only reset counters.
Reset mask: reset only error counters of a specific LID and port.

Syntax:

```
4036-0076(utilities)# perfquery --help
```

```
Usage: perfquery [options]  [<lid|guid> [[port] [reset_mask]]]
```

Options:

```
  --extended, -x          show extended port counters
  --all_ports, -a         show aggregated counters
  --loop_ports, -l        iterate through each port
  --reset_after_read, -r  reset counters after read
  --Reset_only, -R        only reset counters
  --Ca, -C <ca>           Ca name to use
  --Port, -P <port>       Ca port number to use
  --Lid, -L               use LID address argument
  --Guid, -G              use GUID address argument
  --timeout, -t <ms>      timeout in ms
  --sm_port, -s <lid>     SM port lid
  --errors, -e            show send and receive errors
  --verbose, -v           increase verbosity level
  --debug, -d             raise debug level
  --usage, -u             usage message
  --help, -h              help message
  --version, -V           show version
```

Options are detailed in Table 18-1.

Examples:

```
  perfquery              # read local port's performance counters
  perfquery 32 1         # read performance counters from lid 32, port 1
  perfquery -x 32 1      # read extended performance counters from lid 32,
                           port 1
  perfquery -a 32        # read performance counters from lid 32, all ports
  perfquery -r 32 1      # read performance counters and reset
  perfquery -x -r 32 1   # read extended performance counters and reset
  perfquery -R 0x20 1    # reset performance counters of port 1 only
  perfquery -x -R 0x20 1 # reset extended performance counters of port 1
                           only
  perfquery -R -a 32     # reset performance counters of all ports
  perfquery -R 32 2 0x0fff      # reset only error counters of port 2
  perfquery -R 32 2 0xf000      # reset only non-error counters of port 2
```

port-verify

Description: Shows the fabric with the existing errors on each port, if any.

Syntax:

```
4036-0040(utilities)# port-verify -h

Usage: port-verify [options] [topology-file]
```

Options:

```
  --show, -s              show more information
  --list, -l              list of connected nodes
  --grouping, -g          show grouping
```

```
  --Hca_list, -H          list of connected CAs
  --Switch_list, -S       list of connected switches
  --Router_list, -R       list of connected routers
  --node-name-map <file>  node name map file
  --ports, -p             obtain a ports report
  --errors, -e            show errors details
  --Ca, -C <ca>           Ca name to use
  --Port, -P <port>       Ca port number to use
  --timeout, -t <ms>      timeout in ms
  --errors, -e            show errors details
  --verbose, -v           increase verbosity level
  --debug, -d             raise debug level
  --usage, -u             usage message
  --help, -h              help message
  --version, -V           show version
```

Example:

```
4036-0040(utilities)# port-verify
#
# Topology file: generated on Sun Apr 26 13:34:46 2009
#
# Max of 1 hops discovered
# Initiated from node 0008f100010c0040 port 0008f100010c0040

vendid=0x8f1
devid=0x5a5a
sysimgguid=0x8f100010c0041
switchguid=0x8f100010c0040(8f100010c0040)
Switch  36 "S-0008f100010c0040"         # "Voltaire 4036 - 36 QDR ports
switch"                                enhanced port 0 lid 1 lmc 0
[32]    "H-0002c9030002a1aa"[1](2c9030002a1ab)          # "Lian1 HCA-1" lid
16 4                                                    xQDR
[24]    "H-0002c9030002a3ba"[1](2c9030002a3bb)          # "Lian4 HCA-1" lid
64 4                                                    xQDR
XmtDiscards:.....................1

vendid=0x2c9
devid=0x673c
sysimgguid=0x2c9030002a1ad
caguid=0x2c9030002a1aa
Ca      2 "H-0002c9030002a1aa"          # "Lian1 HCA-1"
[1](2c9030002a1ab)      "S-0008f100010c0040"[32]                # lid 16
lmc 0 "                                                 Voltaire 4036 - 36 QDR
ports switch" lid 1 4xQDR
LinkDowned:......................14
XmtDiscards:.....................43

vendid=0x2c9
devid=0x673c
sysimgguid=0x2c9030002a3bd
caguid=0x2c9030002a3ba
Ca      2 "H-0002c9030002a3ba"          # "Lian4 HCA-1"
[1](2c9030002a3bb)      "S-0008f100010c0040"[24]                # lid 64
```

```
lmc 0 "                                                    Voltaire 4036 - 36 QDR
ports switch" lid 1 4xQDR
LinkDowned:.....................18
XmtDiscards:....................57
```

smpquery

Description: Allows a basic subset of standard SMP queries including the following:

node info, node description, switch info, port info. Fields are displayed in human readable format.

Syntax:

```
4036-0076(utilities)# smpquery --help
```

Usage:

```
smpquery [options] <op> <dest dr_path|lid|guid> [op params]

Supported ops (and aliases, case insensitive):
  NodeInfo (NI) <addr>
  NodeDesc (ND) <addr>
  PortInfo (PI) <addr> [<portnum>]
  SwitchInfo (SI) <addr>
  PKeyTable (PKeys) <addr> [<portnum>]
  SL2VLTable (SL2VL) <addr> [<portnum>]
  VLArbitration (VLArb) <addr> [<portnum>]
  GUIDInfo (GI) <addr>
```

Options:

```
  --combined, -c          use Combined route address argument
  --node-name-map <file>  node name map file
  --Ca, -C <ca>           Ca name to use
  --Port, -P <port>       Ca port number to use
  --Direct, -D            use Direct address argument
  --Lid, -L               use LID address argument
  --Guid, -G              use GUID address argument
  --timeout, -t <ms>      timeout in ms
  --sm_port, -s <lid>     SM port lid
  --errors, -e            show send and receive errors
  --verbose, -v           increase verbosity level
  --debug, -d             raise debug level
  --usage, -u             usage message
  --help, -h              help message
  --version, -V           show version
```

Examples:

```
  smpquery portinfo 3 1          # portinfo by lid, with port modifier
  smpquery -G switchinfo 0x2C9000100D051 1      # switchinfo by guid
  smpquery -D nodeinfo 0          # nodeinfo by direct route
  smpquery -c nodeinfo 6 0,12     # nodeinfo by combined route
```

vendstat

Description: vendor specific MAD generator. Queries vendor-specific information of a switch LID.

Syntax:

```
4036-0076(utilities)# vendstat --help
Usage: vendstat [options] <lid|guid>
```

Options:

```
  --N, -N                 show IS3 general information
  --w, -w                 show IS3 port xmit wait counters
  --Ca, -C <ca>           Ca name to use
  --Port, -P <port>       Ca port number to use
  --Lid, -L               use LID address argument
  --Guid, -G              use GUID address argument
  --timeout, -t <ms>      timeout in ms
  --sm_port, -s <lid>     SM port lid
  --errors, -e            show send and receive errors
  --verbose, -v           increase verbosity level
  --debug, -d             raise debug level
  --usage, -u             usage message
  --help, -h              help message
  --version, -V           show version
```

Examples:

```
  vendstat -N 6         # read IS3 general information
  vendstat -w 6         # read IS3 port xmit wait counters
```

19

Chapter 19. Configuration (config) Mode

In This Chapter:

This chapter provides the commands available under the config mode and contains the following sections:

19.1 Overview

Configuration mode commands apply to system-wide features, rather than a specific protocol or interface. From the **config** mode, you can access other CLI modes and menus to configure specific system features, protocols and interfaces. Available commands for each are described under their respective sub-topics.

The Configuration mode command is used to configure advanced parameters.

19.2 Accessing the config Mode

You can access the **config** mode from the Privileged mode by typing config, as shown in the following example.

```
Switch# config
```

19.3 config Mode Command Reference

The commands available in **config** mode and their descriptions are listed below.

```
4036-006E(config)# ?
<command> ?     Displays the command usage string
?               Displays the list of available commands
end             Ends the CLI
exit            Exits to previous menu
factory-default Switches back to factory default, and reboots the system
interface       Changes to interface configuration mode
ntp             Changes to the NPT configuration mode
names           Changes to names configuration mode
ping            Sends ping messages
port            Changes to port configuration mode
remote          Changes to remote configuration mode
security        Changes to security configuration mode
sm              Changes to SM configuration mode
```

The following details the commands available in **config** mode:

factory-default

Description: Reverts the 4036/2036 to its factory default parameter settings and reloads the system. Since this command restores the switch default interfaces IP address, it is important to perform this action via a local terminal in order not to lose communication with the switch.

Syntax: `factory-default`

interface

Description: Changes to Interface configuration mode. This menu enables you to set the management interface and configure the default gateway and DHCP and set the IP and Broadcast addresses.

See section 19.4 for a list of commands available under this menu.

Syntax: `interface`

names

Description: Changes to Names configuration mode, which is used to name or rename the current system name. See section 19.5 for a list of commands available under this menu.

Syntax: `names`

ntp

Description: Changes to the NTP configuration mode. The commands under this menu are currently not supported except for the clock set and clock show commands.

Syntax: `ntp`

port

Description: Changes to port configuration mode. This menu is used to set the ports configurations. See section 19.6 19.6 for a list of commands available under this menu.

Syntax: `port`

remote

Description: Changes to remote configuration mode. See section 0 for a list of commands available under this menu.

Syntax: `remote`

security

Description: Changes to the Security configuration mode. See section 19.9 for a list of commands available under this menu.

Syntax: `security`

sm

Description: Type this command to access the Subnet Manager configuration mode, which is used to set **sm** parameters.

See section 0 for a list of commands available under this menu.

Syntax: `sm`

19.4 Interface Mode

This menu enables you to set the management interface and configure the default gateway and DHCP and set the IP and Broadcast addresses.

The following are the commands available under the Interface menu.

```
2036-0076(config-if)# ?
<command> ?              Displays the command usage string
?                        Displays the list of available commands
broadcast set            Sets the broadcast address
default-gw delete        Deletes the default gateway for the interface
default-gw set           Sets the default gateway for the interface
dhcp set                 Enables/disables the DHCP client
end                      Ends the CLI
exit                     Exits to previous menu
interface ethernet set   Sets Ethernet as the Management interface
interface infiniband set Sets InfiniBand as the Management interface
ip-address set           Sets the interface IP address
ip-address show          Shows the interface IP address and configuration
ping                     Sends ping messages
```

Interface syntax usage is as follows:

```
broadcast set            broadcast set [ip address]
default-gw delete        default-gw delete
default-gw set           default-gw set [ip address]
dhcp set                 dhcp set [disable, enable]
interface ethernet set   interface ethernet set
interface infiniband set interface infiniband set
ip-address set           ip-address set [ip-address] [netmask]
                         [optional broadcast]
ip-address show          ip-address show
```

The following details the commands available under the Interface menu.

IMPORTANT:

You must define the interface according to your needs.

broadcast set

Description: Sets the broadcast address.

Syntax: `broadcast set [ip address]`

Default: The Ethernet default broadcast address is: `192.168.1.255`

The InfiniBand default broadcast address is: `192.168.2.255`

Example:

```
4036-0076(config-if)# broadcast set 172.30.255.255
```

default-gw delete

Description: Deletes the default gateway for the interface.

Syntax: `default-gw delete`

Example:

```
4036-0076(config-if)# default-gw delete
```

default-gw set

Description: Sets the default gateway for the interface.

Syntax: `default-gw set [ip address]`

Default: There is no default gateway. You must define it if required.

Example:

```
4036-0076(config-if)# default-gw set 172.30.0.1
```

dhcp set

Description: Enables/Disables the DHCP client (default: DHCP is enabled)

Syntax: `dhcp set [disable, enable]`

Default: `enable`

Example:

```
4036-0076(config-if)# dhcp set disable
```

interface ethernet set

Description: Sets Ethernet as the Management interface. **Note:** you must first make sure that DHCP is disabled before running this command.

Syntax: `interface ethernet set`

Example:

```
4036-0076(config-if)# interface ethernet set
```

interface infiniband set

Description: Sets the interface IP address.

Syntax: `interface infiniband set`

Example:

```
4036-0076(config-if)# interface infiniband set
```

ip-address set

Description: Sets the interface IP address.

Syntax: `ip-address set [ip-address] [netmask] [optional broadcast]`

Default: The Ethernet default IP address is: `192.168.1.2`

The InfiniBand default IP address is: `192.168.2.100`

Example:

```
4036-0076(config-if)# ip-address set 172.25.3.38 255.255.0.0
```

ip-address show

Description: Shows the interface IP address and configuration.

Syntax: `ip-address show`

Example:

```
4036-0076(config-if)# ip-address show
 port selection     Ethernet
 ip                 172.30.106.122
 mask               255.255.0.0
 broadcast          172.30.255.255
 DHCP client        disabled
 default-gw Ip is:  172.30.0.1
```

19.5 Names Mode

This menu allows you to set up the 4036/2036 name, either set as the unique default name or the preferred user name.

```
4036-0076(config)# names
4036-0076(config-names)# ?
<command> ?               Displays the command usage string
?                         Displays the list of available commands
end                       Ends the CLI
exit                      Exits to previous menu
system-guid show          Shows this computer's system GUID
system-name set           Sets this computer's system name
system-name show          Shows this computer's system name
unique-default-name set   Changes the unique default name option
unique-default-name show  Displays the unique default name option
```

Names syntax usage is as follows:

```
system-guid show            system-guid show
system-name set             system-name set [name]
system-name show            system-name show
unique-default-name set     unique-default-name set [disable, enable]
unique-default-name show    unique-default-name show
```

The following details the commands available under the Names menu:

---

system-guid show

Description: Shows the system guid of this computer.

Syntax: `system-guid show`

Example:

```
4036-0076(config-names)# system-guid show
system guid is 0008f10500100076
```

---

system-name set

Description: Sets the system user-defined name of this computer. Note: in order to run this command, the `unique-default-name set` command must be set to `disable`. The user-defined system name will remain even after reboot.

Syntax: `system-name set [name]`

Default: none

Example:

```
4036-0076(config-names)#
system-name set 4036_New
Change will be effective next time CLI is activated
```

Expected Results:

```
4036-0076 (config-names)# system-name show
system name is 4036_New
```

---

system-name show

Description: Shows the system name of this switch/host.

Syntax: `system-name show`

Default: `enable (unique name)`

Example:

```
4036-0076(config-names)# system-name show
system name is 4036-0076
```

---

unique-default-name set

Description: Enables or disables the unique default name. The unique default name is the name based on the platform name as well as the GUID. For example, a unique default name would look like this: 4036-0076.

If you disable the unique default name, you can set a user-defined system name (see above: system-name set).

The numbers after the dash (in this example: -0076) are the last numbers of the GUID so that the name is unique.

Syntax: `unique-default-name set [disable, enable]`

Default: `enable`

Example:

```
4036-0076(config-names)# unique-default-name set enable
Change will be effective only after next reboot
```

Expected Results:

```
4036-0076(config-names)# unique-default-name show
Enable
```

unique-default-name show

Description: Shows if the unique default name is enabled or disabled.

Syntax: `unique-default-name show`

Example:

```
4036-0076(config-names)# unique-default-name show
enable
```

19.6 NTP Mode

This menu allows you to set and view the local clock.

```
4036-006E(config-ntp)# ?
<command> ?                    Displays the command usage string
?                              Displays the list of available commands
clock set                      Sets the system clock
clock show                     Shows the system clock
end                            Ends the CLI
exit                           Exits to previous menu
ntp server-ip-address set      Sets the NTP server IP address
ntp show                       Shows the NTP attributes
ntp status set                 Sets the NTP status
```

The following details the clock set and clock show commands available under the NTP menu.

---

clock set

Description: Enables you to manually configure the chassis system clock.

Syntax: `clock set MMDDhhmmYYYY[.ss]`

Example:

```
ISR2012-170c(config-ntp)# clock set 042623192007
ISR2012-170c(config-ntp)#
```

Expected Result:

```
ISR2012-170c(config-ntp)# clock show
Thu Apr 26 23:19:07 UTC 2007
```

---

clock show

Description: Shows the chassis system clock.

Syntax: `clock show`

Example:

```
ISR2012-170c(config-ntp)# clock show
Thu Apr 26 23:10:40 UTC 2007
```

19.7 Ports Mode

This menu allows to disable or enable ports (ports are enabled by default). Ports can be disabled if you want to block it for maintenance or if they are faulty.

Note: this configuration is not persistent (needs to be set again after reboot).

The following are the commands available under the Port menu.

```
4036-0076(config-port)# ?
<command> ?     Displays the command usage string
?               Displays the list of available commands
end             Ends the CLI
exit            Exits to previous menu
port set        Enables/disables port.
port state show Shows the port's physical and logical states
```

Port syntax usage is as follows:

```
port set        port set [enable | disable] [port num (1-36)]
port state show port state show
```

The following details the commands available under the Port menu.

---

port set

Description: Enables/Disables port

Syntax: `port set [enable | disable] [port num (1-36)]`

Default: `enable`

Example:

```
4036-0076(config-port)# port set disable 1
```

Expected results are shown in the following command (port down).

NOTE:

This **port set configuration** is not persistent after reboot.

---

port state show

Description: Shows the state of the specific port

Syntax: `port state show [port num (1-36)]`

Example:

```
2036-0076(config-port)# port state show 2
logical state = down
physical state = polling
```

19.8 Remote Mode

This menu allows you to set the remote configurations such as FTP and SCP. You can also use this to backup/export the repository to the Remote Server or save a back it up to flash. In addition, you can upload the logs for support purposes.

IMPORTANT

When exporting a file, make sure to rename a previously exported file on the Remote server in order to avoid overwriting. Please make sure you have writing permissions on the Remote server path.

Configuration may vary according to the Operating System (Linux, Windows, etc.) on which the FTP server and setup are installed.

The following are the commands available under the Remote menu.

```
4036-0076(config-remote)# ?
<command> ?                 Displays the command usage string.
?                           Displays the list of available
                            commands.
copy flash: running-config  Restores the configuration saved from a file
                            in the local repository. The new values will
                            be applied on reboot.
copy remote: running-config Downloads the configuration from the remote
                            server using previously defined server name,
                            user name, and password.
                            The remote path must contain the exported file
                            name. The new values will be applied on reboot.
copy running-config flash:  Saves the configuration file in the local
                            repository. In case of empty name the file name
                            is evaluated by default
copy running-config remote: Uploads the configuration to the remote
                            server using previously defined server name,
                            user name, and password.
                            The remote path can contain the imported file
                            name. If the file name is not indicated, it
                            will be created using a default name.
                            Any characteristic after the last slash in the
                            path will be used as your own defined file
                            name.
end                         Ends the CLI
exit                        Exits to previous menu
exportFile topology         Uploads the Topology File to the remote server
                            using previously defined server name, user
                            name, and password
```

```
exportLOGs                  Uploads Logs to the remote server using
                            previously defined server name, user name, and
                            password
flash delete                Deletes the specific file from flash
flash show                  Shows the configuration files in flash
password                    Sets the user password to access the remote
                            server
protocol set                Sets the protocol to access the remote server
remote show                 Shows the remote client configuration
server                      Sets the remote server ip-address
username                    Sets the user name to access the remote server
```

Remote syntax usage is as follows:

```
copy flash: running-config   copy flash: [file-name] running-config
copy remote: running-config  copy remote: [remote-path] running-config
copy running-config flash:   copy running-config flash: [file-name]
copy running-config remote:  copy running-config remote: [remote-path]
exportFile topology          exportFile topology [remote path]
exportLOGs                   exportLOGs [remote path]
flash delete                 flash delete [file-name]
flash show                   flash show
Password                     password
protocol set                 protocol set [FTP | SCP]
remote show                  remote show
server                       server [ip-address]
username                     username [username]
```

The following details the commands available under the Remote menu.

---

copy flash: running-config

Description: This restores the backup configuration. This command retrieves the repository configuration from a file stored in the Flash, restores it and saves it in the switch repository (database). The new values will be applied on reboot.

Syntax: `copy flash: [file-name] running-config`

Example:

In this example we are using a backup file named JohnDoe and restore it.

```
4036-0076(config-remote)# copy flash: JohnDoe running-config
 New Configuration will take place after Reboot
```

copy remote: running-config

Description: Downloads the configuration from the remote server using previously defined server name, user name, and password.
The remote path must contain the exported file name. The new values will be applied on reboot.

Syntax: `copy remote: [file-name] running-config`

Example:

```
4036-0076(config-remote)# copy remote: /home/avia/ repository 4036-
0076_15_34_2009-01-23_IP_172.30.106.18.new  running-config
New Configuration will take place after Reboot
4036-0076(config-remote)#
```

copy running-config flash:

Description: Backs up the configuration into file in the local repository.

You can back up to two files. Backing up additional files will prompt a message that you are over the limit.

Syntax: `copy running-config flash: [file-name]`

Default: In case of empty name the file name is set by default (example of default format: repository_4036-0076_6_47_2009-01-21_IP_172.30.106.32.new).

Example 1:

In this case, we are running this command without specifying the backup file name. The system will be created using a default backup file name with the following format: repository_4036-0076_6_47_2009-01-21_IP_172.30.106.32.new.

```
4036-0076(config-remote)# copy running-config flash:
Successed to create the file: repository_4036-0076_6_47_2009-01-
21_IP_172.30.106.32.new.
```

Example 2:

In this case, we are running this command with the backup file name (JohnDoe).

```
4036-0076(config-remote)# copy running-config flash: JohnDoe
Successed to create the file: JohnDoe.
```

Example 3:

If you have already two repository backups, you will get the following message if you want to create another one.

```
4036-0076(config-remote)# copy running-config flash:
Failed to create the file: Cannot add another file (maximum: 2 files).
```

copy running-config remote:

Description: Uploads the configuration to the remote server using previously defined server name, user name, and password. The remote path can contain the imported file name. If the file name is not indicated, it will be created using a default name. Any characteristic after the last slash in the path will be used as a user-defined file name.

Syntax: `copy running-config remote: [remote-path].`

Default: In case of empty name the file name is set by default (example of default format: repository_4036-0076_6_47_2009-01-21_IP_172.30.106.32.new).

Example 1:

In this example, the system will upload the configuration to the remote server and will name the file user1. The file will be located under the folder called home.

```
4036-0076(config-remote)# copy running-config remote: /home/user1
```

Expected Result:

```
4036-0076(config-remote)# copy running-config remote: /home/user1
Writing the DB to a repository file...
.........
Exporting the repository file to the remote destination...
Succeeded to create export file: user1.
```

Example 2:

In this example, the system will upload the configuration to the remote server. It will get a default name and will be stored under the folder called /home/user1.

```
 4036-0076(config-remote)# copy running-config remote: /home/user1/
```

Expected Result:

```
4036-0076(config-remote)# copy running-config remote: /home/user1/
Writing the DB to a repository file...
..........
Exporting the repository file to the remote destination...
Succeeded to create export file: repository_4036-0076_12_11_2009-01-
21_IP_172.30.106.18.new.
```

ExportFile topology

Description: Uploads the Topology File to the remote server using previously defined server name, user name, and password.

Syntax: `exportFile topology [remote path].`

Example:

```
4036-0076(config-remote)# exportFile topology /pub/
```

exportLOGs

Description: Uploads Logs to the remote server, using previously defined server name, user name, and password.

Syntax: `exportLOGs [remote path].`

Example:

```
4036-0076(config-remote)# exportLOGs /pub/
```

flash delete

Description: Deletes the specific file from Flash.

Syntax: `flash delete [file-name].`

Example:

```
4036-0076(config-remote)# flash delete JohnDoe
```

Expected Result:

```
4036-0076(config-remote)# flash show
Name
Modification_date
-----------------------------------------------------------|------------------------
repository_4036-0076_7_43_2009-01-21_IP_172.30.106.32.new Mon Jan 21 07:43:07 2009
```

flash show

Description: Shows the configuration files in flash.

Syntax: `flash show.`

Example:

```
4036-0076(config-remote)# flash show

Name                                                        Modification date
------------------------------------------------------------|------------------------
JohnDoe                                                     Mon Jan 21 06:57:14 2009
repository_4036-0076_7_43_2009-01-21_IP_172.30.106.32.new Mon Jan 21 07:43:07 2009
```

Note that the first file name is user defined. In this example, it is called JohnDoe.

The file name in the second example is set by default by the system.

password

Description: Sets the user password to access the remote server.

Syntax: `password.`

Default: none (no password as default, the user must define a password)

Example:

```
4036-0076(config-remote)# password
password: P12345586  <- will be displayed as *****
```

protocol set

Description: Sets the protocol to access the remote server.

Syntax: `protocol set [FTP | SCP]`

Default: FTP

Example:

```
4036-0076(config-remote)# protocol set SCP
```

remote show

Description: Shows the protocol used to access the remote server.

Syntax: `remote show`

Example:

```
4036-0076(config-remote)# remote show
remote configuration
-----------------------
remote server: 172.25.5.152
username:      johnb
protocol:      FTP
```

server

Description: Sets the remote server ip-address.

Syntax: `server [ip-address]`

Example:

```
4036-0076(config-remote)# server 192.34.15.186
```

username

Description: Sets the user name to access remote server (either through FTP or SCP defined by the user to access the remote server).

Syntax: `username [username]`

Example:

```
4036-0076(config-remote)# username Johnb
```

19.9 Security Mode

This menu allows you to set the Security parameters.

The following are the commands available under the Security menu.

```
4036-0076(config-security)# ?
<command> ?     Displays the command usage string
?               Displays the list of available commands
end             Ends the CLI
exit            Exits to previous menu
telnetd set     Sets telnetd option
telnetd show    Shows telnetd option
ufmagent  set   Enables or disables the ufm agent
ufmagent  show  Shows the ufm agent
```

Security syntax usage is as follows:

```
telnetd set                         telnetd set [disable, enable]
telnetd show                        telnetd show
ufmagent  set                       Enables or disables the ufm agent
ufmagent  show                      Shows the ufm agent
```

The following details the commands available under the Security menu.

---

telnetd set

Description: Provides the option to disable telnet for security purposes.

Syntax: `telnetd set [disable, enable]`

Default: enable

Example:

```
Switch(config-security)# telnetd set disable
Change will be effective only after next reboot
```

---

telnetd show

Description: Shows the telnet status.

Syntax: `telnetd show`

Example:

```
4036-0076(config-security)# telnetd show
telnetd   disable
```

ufmagent set

Description: Disables or enables the ufm agent

Syntax: `ufmagent set ufmagent set [enable|disable]`

Default: enable

Example:

```
4036-0076(config-security)# ufmagent  set disable
Change will be effective only after next reboot
```

ufmagent show

Description: Shows the ufm agent

Syntax: `ufmagent show`

Example:

```
4036-0076(config-security)# ufmagent  show
ufmagent mode is disable
```

19.10 SM (Subnet Manager) Mode

The SM menu allows you to configure the parameters of the Subnet Manager.

The following are the commands available under the Subnet Manager menu.

```
4036-0076(config-sm)# ?
<command> ?                    Displays the command usage string
?                              Displays the list of available commands
end                            Ends the CLI
exit                           Exits to previous menu
sm-info babbling_port_policy set
                               Sets babbling_port_policy SM parameter
sm-info head_of_queue_lifetime set
                               Sets transaction_timeout SM parameter
sm-info leaf_head_of_queue_lifetime set
                               Sets leaf_head_of_queue_lifetime SM parameter
sm-info lmc set                Sets LMC SM parameters
sm-info max_op_vls set         Sets max_op_vls SM parameter
sm-info mode set               Enables or disables the subnet manager
                               mechanism.
sm-info packet_life_time set   Sets packet_life_time SM parameter
sm-info polling_retry_number set
                               Sets polling_retry_number SM parameter
sm-info priority set           Sets the priority SM parameters
sm-info reassign_lids set      Sets reassign_lids SM parameter
sm-info routing_engine set     Sets routing_engine SM parameter
sm-info show                   Shows the Subnet Manager (SM) parameters
sm-info sminfo_polling_timeout set
                               Sets sminfo_polling_timeout SM parameter
sm-info sweep_interval set     Sets the sweep_interval SM parameters
```

The following details the SM syntax.

```
sm-info babbling_port_policy set
                               sm-info babbling_port_policy set [disable, enable]
sm-info head_of_queue_lifetime set
                               sm-info head_of_queue_lifetime set [1..19]
                               or [20 ..31 ] for infinite
sm-info leaf_head_of_queue_lifetime set
                               sm-info leaf_head_of_queue_lifetime set [1..19]
                               or [20 ..31 ] for infinite
sm-info lmc set                sm-info lmc set [int (0..7)]
sm-info max_op_vls set         sm-info max_op_vls set [int (0..5)]
sm-info mode set               sm-info mode [enable|disable]
sm-info packet_life_time set   sm-info packet_life_time set [1..19] or
                               [20 ..31 ] for infinite
sm-info polling_retry_number set
                               sm-info polling_retry_number set [int (3..180)]
sm-info priority set           sm-info priority set [int (0..15)]
sm-info reassign_lids set      sm-info reassign_lids set [disable, enable]
```

```
sm-info routing_engine set    sm-info routing_engine set [updn, minhop]
sm-info show                  sm-info show
sm-info sminfo_polling_timeout set
                              sm-info sminfo_polling_timeoutset [int (1000..10000)]
sm-info sweep_interval set    sm-info sweep_interval set [int (2..3600)(seconds)]
```

The following details the commands available under the **SM** menu.

---

sm-info babbling_port_policy set

Description: Sets babbling_port_policy SM parameter. A "babbling" port is a port which causes traps to be frequently generated. It may directly be "this" port which generates the traps or the peer port detecting the issue and that the SMA on switch port 0 generates the traps. This applies to traps 129-131.

Policy

When a bablbing port is detected, the embedded SM will disable the port or its peer switch port (depending on which trap) which should terminate the trap storm.

Detection

250 consecutive traps of this type will be used as the (initial) threshold. The reason for this is so as to not prematurely detect this and disable a port.

Recovery

Admin would reenable port when OK again. (This usually involves rebooting the node causing the trap to be indicated.)

Syntax: `sm-info babbling_port_policy set [disable, enable]`

Default: `Disable`

Example:

```
4036-0076(config-sm)# sm-info babbling_port_policy set enable
```

Expected Result:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
...
...
sm babbling_port_policy = enable
```

sm-info head_of_queue_lifetime set

Description: Sets head_of_queue_lifetime SM parameter. This is the number of sequential packets dropped that cause the port to enter the VLStalled state. This value is for switch ports driving a CA or router port. The result of setting this value to zero is undefined.

Syntax: `sm-info head_of_queue_lifetime set [1..19] or [20 ..31 ] for infinite`

Range: `[1..19] or [20 ..31 ] for infinite`

Default: `0x10`

Example:

```
4036-0076(config-sm)# sm-info head_of_queue_lifetime set 18
```

Expected Result:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
...
...
sm head_of_queue_lifetime = 18
```

sm-info leaf_head_of_queue_lifetime set

Description: Sets leaf_head_of_queue_lifetime SM parameter. The maximal time a packet can wait at the head of queue on switch port connected to a CA or router port.

Syntax: `sm-info leaf_head_of_queue_lifetime set [1..19] or [20 ..31] for infinite`

Range: `[1..19] or [20 ..31 ] for infinite`

Default: `0x10`

Example:

```
4036-0076(config-sm)# sm-info leaf_head_of_queue_lifetime set 16
```

Expected Result:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
...
...
sm leaf_head_of_queue_lifetime = 16
```

sm-info lmc set

Description: Sets LMC SM parameters. Sets the number of LIDs per node in the fabric (a power of 2, from 0 to 7). The LID Mask Control (LMC) allows you to assign more than one LID per port.

Syntax: `sm-info lmc set [int (0..7)]`

Default: LMC=0

Example:

```
4036-0076(config-sm)#sm-info lmc set 3
```

NOTE:

8 (23) LIDS set for every node in the fabric.

Expected Result:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
...
...
sm LMC = 3
```

sm-info max_op_vls set

Description: Sets the maximum number of Virtual Lanes operational on this port. The actual number of VL is the minimum between the switch capability (VLcap) and this parameter set by the user.

max_op_vls are set according to the following:

`0 [No change], 1 [VL0], 2 [VL0-1], 3 [VL0-3], 4 [VL0-7], 5 [VL0-14]`

Syntax: `sm-info max_op_vls set [int (0..5)]`

Range: `0..5`

Default: `5`

Example:

```
4036-0076(config-sm)# sm-info max_op_vls set 5
```

Expected Result:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
...
```

```
...
sm max_op_vls = 5
```

sm-info mode set

Description: Enables or disables the embedded Subnet Manager mechanism**.** When the Subnet Manager is disabled, the 4036/2036 is managed by a Subnet Manager on a remote switch or host on the network (if present).

Syntax: `sm-info mode set [enable|disable]`

Default: enable

Example:

```
4036-0076(config-sm)#sm-info mode set enable
```

Expected Result:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
...
...
sm mode = enable
```

sm-info packet_life_time set

Description: Sets the packet_life_time SM parameter. The code of maximal time a packet can live in a switch. The actual time is 4.096usec * 2^<packet_life_time>. The value 0x14 disables this mechanism

Syntax: `sm-info packet_life_time set [1..19] or [20 ..31 ] for infinite`

Range: `[1..19] or [20 ..31 ] for infinite`

Default: `0x12`

Example:

```
4036-0076(config-sm)# sm-info packet_life_time set 18
```

Expected Result:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
...
...
sm packet_life_time = 18
```

sm-info polling_retry_number set

Description: Sets the polling_retry_number SM parameter. This is the number of

failing polls of remote SM that declares that it dead.

Syntax: `sm-info polling_retry_number set [int (3..180)]`

Range: `3..180`

Default: `12`

Example:

```
4036-0076(config-sm)#sm-info polling_retry_number set 4
```

Expected Result:

```
4036-0076(config-sm)# sm-info show
...
...
sm polling_retry_number = 4
```

---

sm-info priority set

Description: Sets the priority of the Subnet Manager parameters (the higher the number the higher the priority). When there are two Subnet Managers in the network, the one that has the higher priority will be the Master Subnet Manager.

Syntax: `sm-info priority set [int (0..15)]`

Range: `1..15`

Default: `4`

Example:

```
4036-0076(config-sm)# sm-info priority set 14
```

Expected Result:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
...
...
sm priority = 14
```

sm-info reassign_lids set

Description: If enabled, reassigns the LIDs in the fabric. **Note:** You need to restart the sm after setting to enable.

Syntax: `sm-info reassign_lids set [disable, enable]`

Options: `disable, enable`

Default: **`disable`**

Example:

```
4036-0076(config-sm)# sm-info reassign_lids set enable
This configuration will be applied after sm restart (disable/enable).
```

sm-info routing_engine set

Description: Sets routing_engine SM parameter. Sets the routing algorithm to be implemented by the Subnet Manager. The Voltaire Subnet Manager supports the following routing algorithms:

- Up-down algorithm
- Min Hop (Balanced-routing)

Syntax: `sm-info routing_engine set [updn, minhop]`

Options: `updn, minhop`

Default: `minhop`

Example:

```
4036-0076(config-sm)# sm-info routing_engine set updn
```

sm-info show

Description: Shows the Subnet Manager (**sm**) parameters

Syntax: `sm-info show`

Example:

```
4036-0076(config-sm)# sm-info show
subnet manager info is:
sm routing_engine = minhop
sm sweep_interval = 1000
sm max_wire_smps = 4
sm priority = 14
sm LMC = 0
sm max_op_vls = 5
sm transaction_timeout = 200
```

```
sm head_of_queue_lifetime = 18
sm leaf_head_of_queue_lifetime = 16
sm packet_life_time = 18
sm sminfo_polling_timeout = 1000
sm polling_retry_number = 4
sm reassign_lids = disable
sm babbling_port_policy = disable
sm state = standby
sm mode = enable
```

sm-info sminfo_polling_timeout set

Description: Sets sminfo_polling_timeout SM parameter. `Timeout in [msec] between two polls of active master SM`

Syntax: `sm-info sminfo_polling_timeoutset [int (1000..10000)]`

Range: `1000..10000`

Default: `5000`

Example:

```
4036-0076(config-sm)# sm-info sminfo_polling_timeout set 1000
```

sm-info sweep_interval set

Description: Sets the sweep_interval SM parameters. The sweep interval is the number of seconds between subnet sweeps.

Syntax: `sm-info sweep_interval set [int (2..3600)(seconds)]`

Default: `15`

Range: `2..3600`

Example:

```
4036-0076(config-sm)# sm-info sweep_interval set  1000
```

PART 3:

Appendices

Appendix A Acronyms

Acronym	Description
API	Application Programming Interface
ARP	Address Resolution Protocol
CA	Channel Adapter
CBB	Constant bisectional bandwidth
CD	Compact Disk
CLI	Command Line Interface
CPU	Central Processing Unit
CQ	Completion Queues
DMA	Direct Memory Access
FC	Fibre Channel
FE	Fast Ethernet
FTP	File Transfer Protocol
FRU	Field Replaceable Unit
GbE	Gigabit Ethernet
GE	Gigabit Ethernet
GUI	Graphical User Interface
GUID	Global Unique ID
GW	Gateway

Acronym	Description
HCA	Host Channel Adaptor
HPC	High-performance computing
HQ	Head of Queue
IB	InfiniBand
I/O	Input Output
IP	Internet Protocol
ISR	InfiniBand Switch Router
IT	Information Technology
LID	Local ID
LIDSTAT	Properties retrieved from a specific LID
LAN	Local Area Network
LMC	LID Mask Control
MIB	Management Information Base
MTU	Maximum Transmission Level
NAS	Network Attached Storage
OS	Operating System
PM	Performance Monitor
QoS	Quality of Service
QP	Queue pairs
RC	Reliable Connection
RDMA	Remote Direct Memory Access
SAN	Storage Area Network
SA	Subnet Administration
SDP	Socket Direct Protocol
SM	Subnet Manager
SMP	Short for Simple Management Protocol, another name for SNMP2. SNMP2 is an enhanced version of the Simple Network Management Protocol (SNMP) with features required to support larger networks operating at high data transmission rates. SNMP also supports multiple network management workstations organized in a hierarchical fashion.

Acronym	Description
sFU-x	Fan Unit
SCP	(Remote) Secure Copy Protocol
SL	Service Level
SM	Subnet Manager
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	Unreliable Datagram Protocol
DM	Device Manager
VL	Virtual Lane
WQE	Work Queue Elements

Appendix B InfiniBand™ Standard Glossary

Term/Definition/Acronym	Description
Automatic Path Migration	The process in which a Channel Adapter, on a per-Queue Pair basis, signals another CA to cause Path Migration to a preset alternate Path. Automatic Path Migration uses a bit in a request or response packet (MigReq) to signal the other channel adapter to migrate to the predefined alternate path.
Binding	The act of associating a virtual address range in a specified Memory Region with a Memory Window.
Channel	The association of two queue pairs for communication.
Channel Adapter	Device that terminates a link and executes transport-level functions. One of Host Channel Adapter or Target Channel Adapter.
Client	The active entity in an active/passive communication establishment exchange.
Data Payload	The data, not including any control or header information, carried in one packet.
Enhanced Switch Port 0	A Switch Port 0 which provides the functionality of a Target Channel Adapter.
External Switch Port	A physical Port on a Switch. See also Switch Port 0.
Fabric	The collection of Links, Switches, and I/O Gateways that connects a set of Channel Adapters.
Gbps	Giga-bits per second (109 bits per second)
GBps	Giga-bytes per second (109 bytes per second)
GID	See Global Identifier

Term/Definition/Acronym	Description
Global Identifier	A 128-bit identifier used to identify an Endport or a multicast group. GIDs are valid 128-bit IPv6 addresses (per RFC 2373) with additional properties / restrictions defined within IBA to facilitate efficient discovery, communication, and routing.
Globally Unique Identifier	A number that uniquely identifies a device or component.
GUID	See Globally Unique Identifier.
HCA	See Host Channel Adapter.
Host	One or more Host Channel Adapters governed by a single memory/CPU complex.
Host Channel Adapter	A Channel Adapter that supports the Verbs interface.
Initiator	The source of requests.
I/O	Input/Output.
I/O Controller	One of the two architectural divisions of an I/O Unit. An I/O controller (IOC) provides I/O services, while a Target Channel Adapter provides transport services.
I/O Unit	An I/O unit (IOU) provides I/O service(s). An I/O unit consists of one or more I/O Controllers attached to the fabric through a single Target Channel Adapter.
I/O Virtual Address	An address having no direct meaning to the Host processor, intended for use only in describing a Local or Remote memory buffer to the Host Channel Adapter.
Key	A construct used to limit access to one or more resources, similar to a password. The following keys are defined by the InfiniBand architecture: • Baseboard Management Key • Local Key • Management Key • Queue Key • Partition Key • Remote Key
LID	See Local Identifier.
LID Mask Control	A per-port value assigned by the Subnet Manager. The value of the LMC specifies the number of Path Bits in the Local Identifier.
Link	A full duplex transmission path between any two network fabric elements, such as Channel Adapters or Switches.
LMC	See LID Mask Control.

Term/Definition/Acronym	Description
Local Identifier	An address assigned to a port by the Subnet Manager, unique within the subnet, used for directing packets within the subnet. The Source and Destination LIDs are present in the Local Route Header. A Local Identifier is formed by the sum of the Base LID and the value of the Path Bits.
Local Key	An opaque object, created by a verb, referring to a Memory Registration, used with a Virtual Address to describe authorization for the HCA hardware to access local memory. It may also be used by the HCA hardware to identify the appropriate page tables for use in translating virtual to physical addresses.
Local Subnet	The collection of links and Switches that connect the Channel Adapters of a particular subnet.
MAD	See Management Datagram.
Managed Unit	A Unit that provides Vital Product Data about itself to an external entity, and is managed by that entity.
Management Datagram	Refers to the contents of an Unreliable Datagram packet used for communication among HCAs, switches, I/O Gateways, and TCAs to manage the fabric. InfiniBand™ Architecture describes the format of a number of these management commands.
Management Key	A construct that is contained in IBA management datagrams to authenticate the sender to the receiver.
Maximum Transfer Unit	The maximum Packet Payload size, which may be 256, 512, 1024, 2048, or 4096 bytes. See also MTU Capacity, Neighbor MTU, and Path Maximum Transfer Unit.
MB/s	Mega-bytes per second (106 bytes per second)
Memory Protection Attributes	The access rights granted to Memory Regions.
Memory Region	A virtually contiguous area of arbitrary size within a Consumer's address space that has been registered, enabling HCA local access and optional remote access. See Memory Registration
Memory Region Handle	An opaque object returned to the consumer when the consumer registers a Memory Region. The Memory Region Handle is used to specify the registered region to the memory management verbs.
Memory Registration	The act of registering a host Memory Region for use by a consumer. The memory registration operation returns a Memory Region Handle. The process provides this with any reference to a virtual address within the memory region.

Term/Definition/Acronym	Description
Memory Window	An allocated resource that enables remote access after being bound to a specified area within an existing Memory Region. Each Memory Window has an associated Window Handle, set of access privileges, and current R_Key.
Message	A transfer of information between two or more Channel Adapters that consists of one or more packets.
Message-Level Flow Control	See End to End Flow Control.
Message Sequence Number	A value returned as part of an acknowledgement by the responder to the requestor, indicating the last message completed. Contrast Packet Sequence Number.
Modifiers	In a verb definition, the list of input and output objects that specify how, and on what, the verb is to be executed.
MR	Memory Region
MSN	See Message Sequence Number.
MTU	See Maximum Transfer Unit.
MTUCap	See MTU Capacity.
MTU Capacity	The largest Maximum Transfer Unit that a port can support.
Multicast	A facility by which a packet sent to a single address may be delivered to multiple ports.
Multicast Identifier	A Local Identifier or Global Identifier for a Multicast Group. Multicast Group A collection of Endports that receive Multicast packets sent to a single address.
MW	Memory Window
Neighbor MTU	The configured Maximum Transfer Unit for a Port, the value that specifies the maximum packet payload that may be sent to, or received from, the port at the other end of the Link.
NQ	Notification Queue.
Out-of-band Management	Management messages which traverse a transport other than the InfiniBand™ fabric.
Outstanding	1) The state of a Work Request after it has been posted on a Work Queue, but before the retrieval of the Work Completion by the consumer. 2) The state of a packet that has been sent onto the fabric but has not been acknowledged.
P_Key	See Partition Key.

Term/Definition/Acronym	Description
Packet	The indivisible unit of IBA data transfer and routing, consisting of one or more headers, a Packet Payload, and one or two CRCs.
Packet Payload	The portion of a Packet between (not including) any Transport header(s) and the CRCs at the end of each packet. The packet payload contains up to 4096 bytes.
Packet Sequence Number	A value carried in the Base Transport Header that allows the detection and re-sending of lost packets.
Partition	A collection of Channel Adapter ports that are allowed to communicate with one another. Ports may be members of multiple partitions simultaneously. Ports in different partitions are unaware of each other's presence insofar as possible.
Partition Key	A value carried in packets and stored in Channel Adapters that is used to determine membership in a partition.
Default Partition Key:	A partition key special value providing Full membership in the default partition. See Partition Membership Type.
Invalid Partition Key:	A special value that indicates that the Partition Key Table entry does not contain a valid key.
Partition Key Table	A table of partition keys present in each Port.
Partition Key Table Index (P_Key_ix)	An index into the partition key table.
Partition Manager	The entity that manages partition keys and membership.
Partition Membership Type	The high-order bit of the partition key is used to record the type of membership in an Port's partition table: 0 for Limited, 1 for Full. Limited members cannot accept information from other Limited members, but communication is allowed between every other combination of membership types.
Peer	1) One of the agents in an active/active connection establishment exchange. 2) A generic term for the entity at the other end of a connection.
PM	See Partition Manager.
QoS	See Quality of Service.
Quality of Service	Metrics that predict the behavior, reliability, speed, and latency of a given network connection.
RDMA	See Remote Direct Memory Access.

Term/Definition/Acronym	Description
Remote Direct Memory Access	Method of accessing memory on a remote system without interrupting the processing of the CPU(s) on that system.
Remote Key	An opaque object, created by a verb, referring to a Memory Region or Memory Window, used with a Virtual Address to describe authorization for the remote device to access local memory. It may also be used by the HCA hardware to identify the appropriate page tables for use in translating virtual to physical addresses.
Router	A device that transports packets between IBA subnets.
SA	See Subnet Administration.
SCP	Secure Copy Protocol is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol.
Server	1) The passive entity in a connection establishment exchange. 2) An entity (e.g., a process) that provides services in response to requests from clients.
Subnet	A set of InfiniBand™ Architecture Ports, and associated links, that have a common Subnet ID and are managed by a common Subnet Manager. Subnets may be connected to each other through routers.
Subnet Administration	The architectural construct that implements the interface for querying and manipulating subnet management data.
Subnet Manager	One of several entities involved in the configuration and control of the subnet.
Master Subnet Manager	The subnet manager that is authoritative, that has the reference configuration information for the subnet.
Standby Subnet Manager	A subnet manager that is currently quiescent, and not in the role of a master SM, by agency of the master SM. Standby SMs are dormant managers.
Subnet Management Agent	An entity present in all IBA Channel Adapters and Switches that processes Subnet Management Packets from Subnet Manager(s).
Subnet Management Data	Vital Product Data required by the Subnet Manager.
Subnet Management Packet	The subclass of Management Datagrams used to manage the subnet. SMPs travel exclusively over Virtual Lane 15 and are addressed exclusively to Queue Pair Number 0.
Switch	A device that routes packets from one link to another of the same Subnet, using the Destination Local Identifier field in the Local Route Header.
Switch Management Port	A virtual port by which a Switch may be managed. See Switch Port 0.

Term/Definition/Acronym	Description
Switch Port 0	An addressable virtual port by which a Switch may be managed. May be one of Base Switch Port 0 or Endport.
TCA	See Target Channel Adapter.
Target Channel Adapter	A Channel Adapter typically used to support I/O devices. TCAs are not required to support the Verbs interface. See also I/O Unit.
Transport Service Type	Describes the reliability, sequencing, message size, and operation types that will be used between the communicating Channel Adapters. Transport service types that use the IBA transport.
Unicast	An identifier for a single port. A packet sent to a unicast address is delivered to the port identified by that address.
Unit	One or more sets of processes and/or functions attached to the fabric by one or more channel adapters. See Host and I/O Unit.
Unreliable Connection	A Transport Service Type in which a Queue Pair is associated with only one other QP, such that messages transmitted by the send queue of one QP are, if delivered, delivered to the receive queue of the other QP. As such, each QP is said to be “connected” to the opposite QP. Messages with errors are not retried by the transport, and error handling must be provided by a higher level protocol.
Virtual Lane	A method of providing independent data streams on the same physical link.
Vital Product Data	Device-specific data to support management functions.
VL	See Virtual Lane.
VPD	See Vital Product Data.

www.voltaire.com

Business Headquarters
Voltaire Inc.
6 Fortune Drive, Suite 301
Billerica, MA
USA 01821
Tel: 978-439-5400
Fax: 978-439-5401

R&D Center
Voltaire, Ltd.
13 Zarchin St
Raanana 43662
Israel
Tel: +972-74-7129000
Fax: +972-74-7129111

VOLTAIRE