

# Network OS Administration Guide

Supporting Network OS 7.0.0

© 2016, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, ClearLink, DCX, Fabric OS, HyperEdge, ICX, MLX, MyBrocade, OpenScript, VCS, VDX, Vplane, and Vyatta are registered trademarks, and Fabric Vision is a trademark of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

# Contents

---

<b>Preface</b> .....	<b>11</b>
Document conventions.....	11
Text formatting conventions.....	11
Command syntax conventions.....	11
Notes, cautions, and warnings.....	12
Brocade resources.....	12
Contacting Brocade Technical Support.....	12
Brocade customers.....	12
Brocade OEM customers.....	13
Document feedback.....	13
<b>About This Document</b> .....	<b>15</b>
Supported hardware and software.....	15
Using the Network OS CLI .....	15
What's new in this document.....	15
<b>Introduction to Data Center Fabric</b> .....	<b>17</b>
Data Center Fabric overview.....	17
Brocade Data Center Fabric terminology.....	17
<b>VCS Fabrics</b> .....	<b>19</b>
VCS Fabrics overview.....	19
Brocade VCS Fabric terminology.....	21
Automation.....	21
Distributed intelligence.....	22
Logical chassis.....	23
Ethernet fabric formation.....	24
Brocade VCS Fabrics technology use cases.....	25
Classic Ethernet access and aggregation use case.....	25
Large-scale server virtualization use case.....	27
Brocade VCS Fabric connectivity with Fibre Channel SAN.....	28
Topology and scaling.....	28
Core-edge topology.....	29
Ring topology.....	30
Full mesh topology.....	30
Fabric overview.....	31
Brocade VCS Fabric formation.....	32
How RBridges work.....	32
Neighbor discovery.....	33
Brocade trunks.....	33
Fabric formation.....	34
Fabric routing protocol .....	34
Configuring a Brocade VCS Fabric.....	34
Adding a new switch into a fabric.....	36
Configuring fabric interfaces.....	36
Configuring broadcast, unknown unicast, and multicast forwarding.....	37
Configuring VCS virtual IP addresses.....	38
Configuring fabric ECMP load balancing.....	40

<b>Basic Switch Management.....</b>	<b>43</b>
Switch management overview.....	43
Connecting to a switch.....	43
Telnet and SSH.....	43
SSH server key exchange and authentication.....	44
Feature support for Telnet.....	44
Feature support for SSH.....	45
Telnet and SSH considerations and limitations.....	45
Using DHCP Automatic Deployment.....	45
DHCP zero touch provisioning.....	54
Ethernet management interfaces.....	55
Brocade VDX Ethernet interfaces.....	55
Lights-out management.....	56
Stateless IPv6 autoconfiguration.....	56
Switch attributes.....	56
Switch types.....	56
Operational modes.....	57
Logical chassis cluster mode.....	58
Fabric cluster mode (VCS Fabrics only).....	60
Transitioning between modes (VCS Fabrics only).....	61
Modular platform basics.....	61
Management modules.....	62
Switch fabric modules.....	63
Line cards.....	63
Supported interface modes.....	63
Slot numbering and configuration.....	64
Slot numbering.....	64
Slot configuration.....	64
Connecting to a switch.....	64
Establishing a physical connection for a Telnet or SSH session.....	64
Telnet services.....	65
Connecting with SSH.....	66
Using the management VRF.....	68
Configuring and managing switches.....	68
Configuring Ethernet management interfaces.....	68
Configuring a switch in logical chassis cluster mode.....	74
Configuring a switch in fabric cluster mode.....	84
Displaying switch interfaces.....	84
Displaying slots and module status information.....	85
Replacing a line card .....	86
Configuring High Availability.....	87
Disabling and enabling a chassis.....	88
Rebooting a switch.....	88
Troubleshooting switches.....	89
Configuring policy-based resource management and hardware profiles.....	91
Configuring KAP profiles.....	91
Configuring route-table profiles.....	94
Configuring TCAM profiles.....	95
Guidelines for changing hardware profiles.....	97
Using hardware profile show commands.....	98

Hardware-profile upgrade/downgrade considerations.....	98
Auto Fabric.....	99
Configuring Auto Fabric for bare metal.....	99
Changing RBridge-ID-to-WWN mapping for bare-metal configuration.....	100
Using maintenance mode for graceful traffic diversion (VCS Fabrics only).....	101
Overview of maintenance mode.....	101
Configuring maintenance mode.....	105
Tunable SFP+ optics.....	106
Configuring tunable SFP+ optics.....	107
Tunable SFP+ optics channels.....	108
<b>Network Time Protocol.....</b>	<b>111</b>
Network Time Protocol overview.....	111
Date and time settings.....	111
Time zone settings.....	111
Configuring NTP.....	111
Configuration considerations for NTP.....	111
Setting the date and time.....	112
Setting the time zone.....	112
Displaying the current local clock and time zone.....	113
Removing the time zone setting.....	113
Synchronizing the local time with an external source.....	113
Displaying the active NTP server.....	113
Removing an NTP server IP address.....	114
Authenticating NTP.....	114
<b>Configuration Management.....</b>	<b>115</b>
Configuration management overview.....	115
Configuration file types.....	115
Displaying configurations.....	116
Displaying the default configuration.....	116
Displaying the startup configuration.....	117
Displaying the running configuration.....	117
Saving configuration changes.....	117
Saving the running configuration.....	117
Saving the running configuration to a file.....	117
Applying previously saved configuration changes.....	118
Backing up configurations.....	118
Uploading the startup configuration to an external host.....	118
Backing up the startup configuration to a USB device.....	118
Configuration restoration.....	119
Restoring the default configuration.....	119
Managing configurations on a modular chassis.....	119
Managing configurations on line cards.....	120
Managing configurations across redundant management modules.....	120
Managing configurations in Brocade VCS Fabric mode.....	120
Automatic distribution of configuration parameters.....	121
Downloading a configuration to multiple switches.....	121
Rejoining an offline node to a logical chassis cluster.....	121
Using default configuration in logical chassis cluster to avoid segmentation issues.....	122
Managing flash files.....	122

Listing the contents of the flash memory.....	123
Deleting a file from the flash memory.....	123
Renaming a flash memory file.....	123
Viewing the contents of a file in the flash memory.....	123
<b>SNMP.....</b>	<b>125</b>
Simple Network Management Protocol overview.....	125
SNMP Manager.....	125
SNMP Agent.....	125
Management Information Base (MIB).....	125
Basic SNMP operation.....	125
SNMP configuration.....	126
Configuring SNMP community strings.....	127
Configuring SNMP server hosts.....	128
Configuring multiple SNMP server context to VRF mapping.....	129
Configuring SNMP server views.....	130
Configuring SNMP server groups.....	131
Configuring SNMP server users.....	132
Configuring SNMP server v3hosts.....	133
Managing SNMP access rights using ACLs.....	133
Displaying SNMP configurations.....	135
Enabling and disabling SNMP server trap link-status.....	135
Enabling and disabling the SNMP server offline-if enable.....	136
Configuring tuple representation for IF-MIB objects.....	136
<b>Metro VCS.....</b>	<b>137</b>
Metro VCS overview.....	137
Metro VCS details and configuration.....	137
Metro VCS using long-distance ISLs.....	139
Metro VCS using standard-distance ISLs.....	141
Metro VCS combined with vLAGs.....	143
Configuring a long-distance ISL.....	145
Configuring interconnected Ethernet Fabrics.....	146
Using Diagnostic Port for link traffic tests.....	148
<b>Zones.....</b>	<b>149</b>
Zoning overview.....	149
Example zoning topology.....	149
LSAN zones.....	151
Managing domain IDs.....	152
Approaches to zoning.....	153
Zone objects.....	153
Zoning enforcement.....	154
Considerations for zoning architecture.....	155
Operational considerations for zoning.....	155
Configuring and managing zones.....	156
Zone configuration management overview.....	156
Understanding and managing default zoning access modes.....	157
Managing zone aliases.....	158
Creating zones.....	160
Managing zones.....	163
Zone configuration scenario example.....	169

Merging zones.....	171
Configuring LSAN zones: Device-sharing example.....	175
<b>Configuring Fibre Channel Ports.....</b>	<b>181</b>
Fibre Channel ports overview.....	181
Connecting to an FC Fabric through an FC Router.....	182
Fibre Channel port configuration.....	182
Using Fibre Channel commands.....	182
Activating and deactivating Fibre Channel ports.....	183
Configuring and viewing Fibre Channel port attributes.....	184
Configuring a Fibre Channel port for trunking.....	186
Monitoring Fibre Channel ports.....	186
<b>Access Gateway.....</b>	<b>189</b>
Access Gateway basic concepts.....	189
Switches supported for Access Gateway.....	189
Network diagrams.....	190
Access Gateway and native VCS modes.....	192
Access Gateway in a logical chassis cluster.....	193
Access Gateway with FCoE logical SANs.....	193
Access Gateway ports.....	193
Access Gateway features and requirements.....	196
Enabling Access Gateway mode.....	199
Disabling Access Gateway mode.....	199
Displaying Access Gateway configuration data.....	200
VF_Port to N_Port mapping.....	202
Displaying port mapping.....	202
Configuring port mapping.....	203
Port Grouping policy.....	205
Displaying port grouping information.....	206
Creating and removing port groups.....	206
Naming a port group.....	207
Adding and removing N_Ports in a port group.....	208
Port Grouping policy modes.....	209
Trunking in Access Gateway mode.....	211
Setting up trunking for Access Gateway.....	212
Access Gateway under FlexPort.....	212
Configuring Access Gateway under FlexPort.....	212
Restoring N_Port login balance.....	213
N_Port monitoring for unreliable links.....	213
Setting and displaying the reliability counter for N_Port monitoring.....	213
Displaying Access Gateway N_Port utilization data.....	214
<b>System Monitor and Threshold Monitor.....</b>	<b>215</b>
System Monitor overview.....	215
Monitored components.....	215
Monitored FRUs.....	215
Configuring System Monitor.....	216
Setting system thresholds.....	216
Setting state alerts and actions.....	217
Configuring e-mail alerts.....	217
Viewing system SFP optical monitoring defaults.....	218

Displaying the switch health status.....	218
Threshold Monitor overview.....	218
CPU and memory monitoring.....	218
SFP monitoring.....	219
Security monitoring.....	221
Interface monitoring.....	221
Configuring Threshold Monitor.....	222
Viewing threshold status.....	222
CPU and memory threshold monitoring.....	222
Configuring SFP monitoring thresholds and alerts.....	223
Security monitoring.....	224
Configuring Interface monitoring.....	224
Pausing and continuing threshold monitoring.....	225
<b>VMware vCenter .....</b>	<b>227</b>
vCenter and Network OS integration overview.....	227
vCenter properties.....	227
vCenter guidelines and restrictions.....	227
vCenter discovery.....	228
vCenter configuration.....	228
Step 1: Enabling QoS.....	228
Step 2: Enabling CDP/LLDP .....	229
Step 3: Adding and activating the vCenter.....	229
Discovery timer interval .....	230
User-triggered vCenter discovery.....	230
Viewing the discovered virtual assets.....	231
<b>Overview of OpenStack.....</b>	<b>233</b>
OpenStack L2 Gateway.....	234
<b>Configuring Support for OpenStack.....</b>	<b>237</b>
Configuring OpenStack to access Network OS.....	237
Configuring OpenStack support for Layer 2 gateways.....	237
Configuring OpenStack support for Layer 2 population.....	238
Configuring a Layer 2 gateway to connect as an OpenStack SSL client.....	239
Configuring a VDX as an OVSDDB SSL server for OpenStack.....	239
<b>Remote Monitoring.....</b>	<b>243</b>
RMON overview.....	243
Configuring and managing RMON.....	243
Configuring RMON events.....	243
Configuring RMON Ethernet group statistics collection.....	243
Configuring RMON alarm settings.....	244
Monitoring CRC errors.....	245
<b>Diagnostic Port.....</b>	<b>247</b>
Supported platforms for D_Port.....	247
Understanding D_Port.....	247
D_Port configuration modes and testing.....	248
General limitations and considerations for D_Port tests.....	249
Topology 1: ISLs.....	250
Using D_Port in static-static mode between switches.....	250
Enabling D_Port in static mode.....	250



Disabling D_Port in static mode.....	252
Disabling D_Port globally.....	253
Using D_Port in dynamic mode.....	253
Enabling D_Port in dynamic mode.....	253
Disabling D_Port in dynamic mode.....	254
Managing D_Port testing.....	255
Using D_Port show commands.....	255
<b>Python Event-Management and Scripting.....</b>	<b>259</b>
Python under Network OS .....	259
Python overview .....	259
Working interactively in the Python shell .....	259
Implementing Python scripts .....	260
Guidelines for writing Python scripts .....	261
Testing Python-script statements .....	261
Copying Python files to switches .....	261
Running Python scripts from the command line.....	262
Python scripts and run-logs .....	263
Implementing Python event-management .....	269
Configuring an event-handler profile .....	270
Activating an event-handler on an RBridge .....	270
Configuring event-handler options .....	271
Troubleshooting event-management.....	272
Aborting an event-handler action.....	272
Event-management show commands .....	272



# Preface

---

- Document conventions..... 11
- Brocade resources..... 12
- Contacting Brocade Technical Support..... 12
- Document feedback..... 13

## Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

## Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
<b>bold text</b>	Identifies command names Identifies keywords and operands Identifies the names of user-manipulated GUI elements
<i>italic text</i>	Identifies text to enter at the GUI Identifies emphasis Identifies variables
Courier font	Identifies document titles Identifies CLI output Identifies command syntax examples

## Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, <b>--show</b> WWN.
[ ]	Syntax components displayed within square brackets are optional.
{ x   y   z }	Default responses to system prompts are enclosed in square brackets. A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x   y	In Fibre Channel products, square brackets may be used instead for this purpose. A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.

Convention	Description
...	Repeat the previous element, for example, <i>member{member...}</i> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

## Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

### NOTE

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

### ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.



### CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



### DANGER

*A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.*

## Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at [www.brocade.com](http://www.brocade.com). Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to [MyBrocade](http://MyBrocade). You can register at no cost to obtain a user ID and password.

Release notes are available on [MyBrocade](http://MyBrocade) under Product Downloads.

White papers, online demonstrations, and data sheets are available through the [Brocade website](http://Brocade website).

## Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

## Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to <http://www.brocade.com/services-support/index.html>.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: <ul style="list-style-type: none"> <li>• <a href="#">My Cases</a> through MyBrocade</li> <li>• <a href="#">Software downloads</a> and licensing tools</li> <li>• <a href="#">Knowledge Base</a></li> </ul>	Required for Sev 1-Critical and Sev 2-High issues: <ul style="list-style-type: none"> <li>• Continental US: 1-800-752-8061</li> <li>• Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33)</li> <li>• For areas unable to access toll free number: +1-408-333-6061</li> <li>• <a href="#">Toll-free numbers</a> are available in many countries.</li> </ul>	<a href="mailto:support@brocade.com">support@brocade.com</a> Please include: <ul style="list-style-type: none"> <li>• Problem summary</li> <li>• Serial number</li> <li>• Installation details</li> <li>• Environment description</li> </ul>

## Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

## Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on [www.brocade.com](http://www.brocade.com).
- By sending your feedback to [documentation@brocade.com](mailto:documentation@brocade.com).

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



# About This Document

---

- Supported hardware and software.....15
- Using the Network OS CLI .....15
- What's new in this document.....15

## Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Network OS, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Network OS:

- Brocade VDX 2741
- Brocade VDX 2746
- Brocade VDX 6740
  - Brocade VDX 6740-48
  - Brocade VDX 6740-64
- Brocade VDX 6740T
  - Brocade VDX 6740T-48
  - Brocade VDX 6740T-64
  - Brocade VDX 6740T-1G
- Brocade VDX 6940-36Q
- Brocade VDX 6940-144S
- Brocade VDX 8770
  - Brocade VDX 8770-4
  - Brocade VDX 8770-8

To obtain information about a Network OS version other than this release, refer to the documentation specific to that version.

## Using the Network OS CLI

For complete instructions and support for using the Network OS command line interface (CLI), refer to the *Network OS Command Reference*.

## What's new in this document

This document supports the following features introduced in Network OSv7.0.0:

- Introduction to IP Fabrics, a newly supported type of Brocade fabric, that, along with VCS Fabrics, are part of Brocade Data Center Fabrics.
- A new DHCP client identifier definition and support for a single DAD configuration file per IP Fabric for DHCP auto-deployment has been introduced.

- Diagnostic port on TRILL ISLs.
- Dual-personality ports, which allow you to configure supported front-end ports in 40G or 100G mode.
- Maintenance mode, which allows a switch to remain part of the fabric during maintenance while traffic gets diverted through the other switches in the fabric.
- Tunable SFP+ Optics, which support a new type of flexible-wavelength optical transceiver module.

For complete information, refer to the *Network OS Release Notes*.



# Introduction to Data Center Fabric

- [Data Center Fabric overview](#).....17
- [Brocade Data Center Fabric terminology](#).....17

## Data Center Fabric overview

Brocade Network OS is a scalable network operating system available for the Brocade data center switching portfolio products, including the VDX product line. While a Data Center Fabric can refer to many combinations of Ethernet and Fibre Channel networks working in concert, the Network OS Data Center fabrics comprise VCS Fabrics and IP Fabrics.

A Network OS VCS Fabric is a topologically flat network of Ethernet switches with shared intelligence. The VCS Fabric topology is designed for classic hierarchical Ethernet architecture with the same data center as a Brocade VCS Fabric architecture. For detailed information, refer to the "VCS Fabrics" chapter. A VCS Fabric is sometimes referred to as an "Ethernet Fabric." In general, the concept of RBridge ID management, principal nodes, TRILL, and ISLs are concepts that pertain to a VCS Fabric.

A Network OS IP Fabric is a specialized spine-leaf topology of Ethernet switches with shared intelligence. The IP Fabric topology is designed for high-redundancy of network paths without large differences in transmission times. For detailed information, refer to the *Network OS IP Fabrics Configuration Guide*. Also, refer to the Brocade IP Fabrics Data sheet, which includes a list of features supported in a Brocade IP Fabric.

Purpose-built for mission-critical, next-generation data centers, Network OS Data Center fabrics supports the following capabilities:

Simplified network management	Brocade Virtual Cluster Switching (VCS) fabrics are self-forming and self-healing, providing an operationally scalable foundation for very large or dynamic cloud deployments. Multi-node fabrics can be managed as a single logical element, and fabrics can be deployed and easily re-deployed in a variety of configurations optimized to the needs of particular workloads.
Server Virtualization	Automatic Migration of Port Profile (AMPP) functionality provides fabric-wide configuration of network policies, achieves per-port profile forwarding, and enables network-level features to support Virtual Machine (VM) mobility.  Refer to the "Configuring AMPP section" of the <i>Network OS Layer 2 Switching Configuration Guide</i> for more information about AMPP.
Network convergence	Data Center Bridging (DCB)-based lossless Ethernet service provides isolation between IP and storage traffic over a unified network infrastructure. Multi-hop Fibre Channel over Ethernet (FCoE) allows an FCoE initiator to communicate with an FCoE target that is a number of hops away.  Refer to the "End-to-end FCoE" section of the <i>Network OS Layer 2 Switching Configuration Guide</i> for more information about multi-hop FCoE.

In Network OS, most features are configured through a single, industry-standard command line interface (CLI). Refer to the *Network OS Command Reference* for an alphabetical listing and detailed description of all the Network OS commands.

## Brocade Data Center Fabric terminology

The following terms are used in this document.

**TABLE 2** Brocade Data Center Fabric terms

Term	Definition
Edge ports	In an Ethernet fabric, all switch ports used to connect external equipment, including end stations, switches, and routers.

**TABLE 2** Brocade Data Center Fabric terms (continued)

Term	Definition
ESI	Ethernet Segment Identifier - If a customer edge (CE) is multi-homed to two or more provider edges (PE), the set of Ethernet links that attaches the CE to the PEs is called an 'Ethernet segment'. Ethernet segments MUST have a unique non-zero identifier.
Ethernet fabric	A topologically flat network of Ethernet switches with shared intelligence, such as the Brocade VCS Fabric.
EVI	An EVPN instance spanning across the provider edges participating in that EVPN.
EVPN	An Ethernet Virtual Private Network that connects remote sites using a Layer 2 virtual bridge.
Fabric ports	The ports on either end of an Inter-Switch Link (ISL) in an Ethernet fabric.
Inter-Switch Link (ISL)	An interface connected between switches in a VCS fabric. The ports on either end of the interface are called ISL ports or Fabric ports. The ISL can be a single link or a bundle of links forming a Brocade trunk. This trunk can either be created as a proprietary Brocade trunk, or a standard IEEE 802.3ad based link aggregation.
IP Fabric	A spine-leaf network configuration in which each spine is physically connected to each leaf, and each leaf is physically connected to each spine. There is no physical connectivity from spine to spine or leaf to leaf, however.
RBridge	A physical switch in a VCS Fabric.
VCS Fabric	A topologically flat network of Ethernet switches with shared intelligence.
VCS ID	A unique identifier for a VCS fabric. The factory default VCS ID is 1. All switches in a VCS Fabric must have the same VCS ID.
WWN	World Wide Name. A globally unique ID that is burned into the switch at the factory.

# VCS Fabrics

---

• VCS Fabrics overview.....	19
• Brocade VCS Fabrics technology use cases.....	25
• Topology and scaling.....	28
• Fabric overview.....	31
• Configuring a Brocade VCS Fabric.....	34

## VCS Fabrics overview

Brocade VCS Fabrics technology is an Ethernet technology that allows you to create flatter, virtualized, and converged data center networks. Brocade VCS Fabrics technology is elastic, permitting you to start small, typically at the access layer, and expand your network at your own pace.

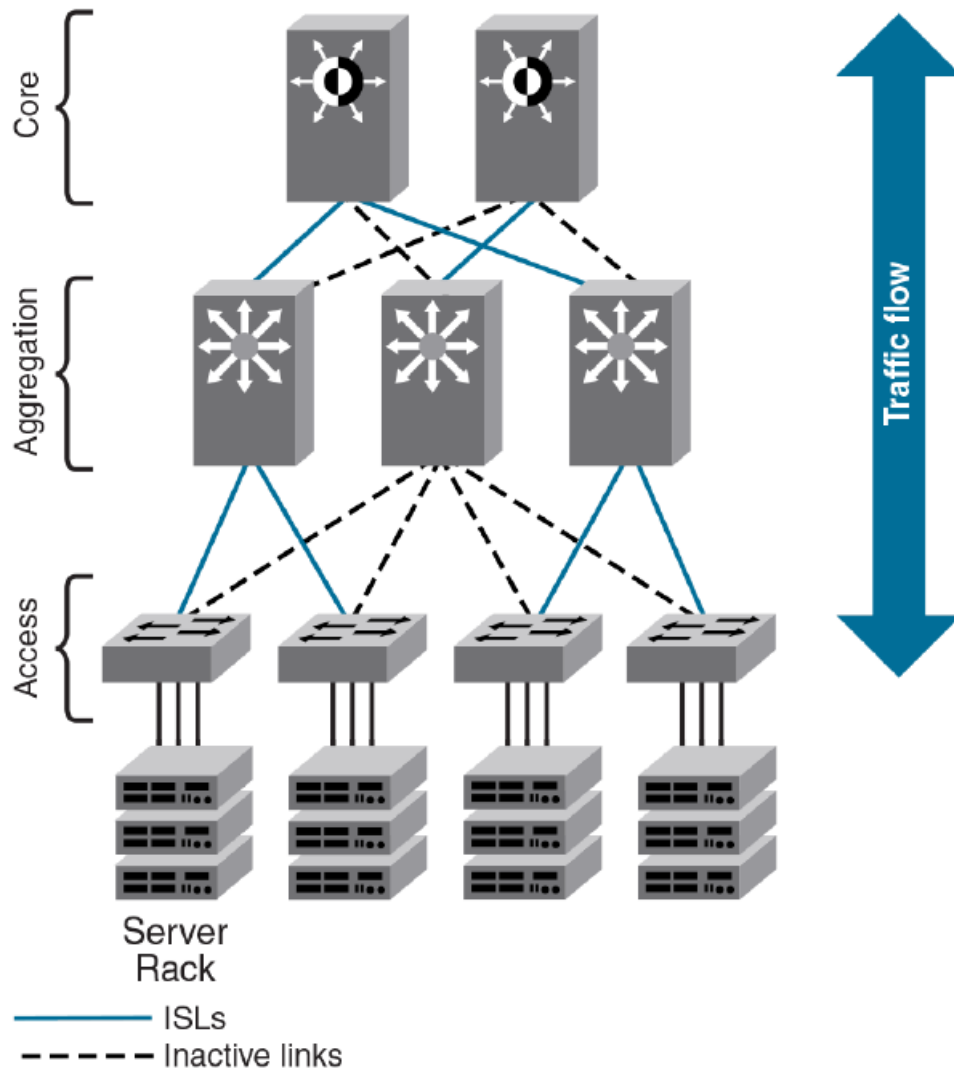
Brocade VCS Fabrics technology is built upon three core design principles:

- Automation
- Resilience
- Evolutionary design

When two or more Brocade VCS Fabrics switches are connected together, they form an *Ethernet fabric* and exchange information among each other using *distributed intelligence*. To the rest of the network, the Ethernet fabric appears as a single *logical chassis*.

The following figure shows an example of a data center with a classic hierarchical Ethernet architecture and the same data center with a Brocade VCS Fabrics architecture. The Brocade VCS Fabrics architecture provides a simpler core-edge topology and is easily scalable as you add more server racks.

FIGURE 1 Classic Ethernet architecture



In addition to the standard Data Center Fabrics capabilities, VCS Fabrics provide the capabilities listed in the following table.

High resiliency	Brocade VCS fabrics use hardware-based Inter-Switch Link (ISL) Trunking to provide automatic link failover without traffic interruption.
Improved network utilization	<p>Transparent Interconnection of Lots of Links (TRILL)-based Layer 2 routing service provides equal-cost multipaths in the network, resulting in improved network utilization. Brocade VCS Fabric technology also delivers multiple active, fully load-balanced Layer 3 gateways to remove constraints on Layer 2 domain growth, eliminate traffic tromboning, and enable inter-VLAN routing within the fabric.</p> <p>Virtual Router Redundancy Protocol (VRRP) eliminates a single point of failure in a static, default-route environment by dynamically assigning virtual IP routers to participating hosts. The interfaces of all routers in a virtual router must belong to the same IP subnet. There is no restriction</p>

against reusing a virtual router ID (VRID) with a different address mapping on different LANs.

Refer to [Fabric overview](#) on page 31 for additional information about TRILL.

Refer to the "VRRP overview" section of the *Network OS Layer 3 Routing Configuration Guide* for additional information on VRRP/VRRP-E.

## Brocade VCS Fabric terminology

The following terms are used in this document.

**TABLE 4** Network OS terms

Term	Definition
Edge ports	In an Ethernet fabric, all switch ports used to connect external equipment, including end stations, switches, and routers.
Ethernet fabric	A topologically flat network of Ethernet switches with shared intelligence, such as the Brocade VCS Fabric.
Fabric ports	The ports on either end of an Inter-Switch Link (ISL) in an Ethernet fabric.
Inter-Switch Link (ISL)	An interface connected between switches in a VCS fabric. The ports on either end of the interface are called ISL ports or Fabric ports. The ISL can be a single link or a bundle of links forming a Brocade trunk. This trunk can either be created as a proprietary Brocade trunk, or a standard IEEE 802.3ad based link aggregation.
RBridge	A physical switch in a VCS fabric.
RBridge ID	A unique identifier for an RBridge, each switch has a unique RBridge ID. In commands, the RBridge ID is used in referencing all interfaces in the VCS fabric. Refer to <a href="#">Configuring a Brocade VCS Fabric</a> on page 34 for information about setting the RBridge ID.
VCS ID	A unique identifier for a VCS fabric. The factory default VCS ID is 1. All switches in a VCS fabric must have the same VCS ID.
WWN	World Wide Name. A globally unique ID that is burned into the switch at the factory.

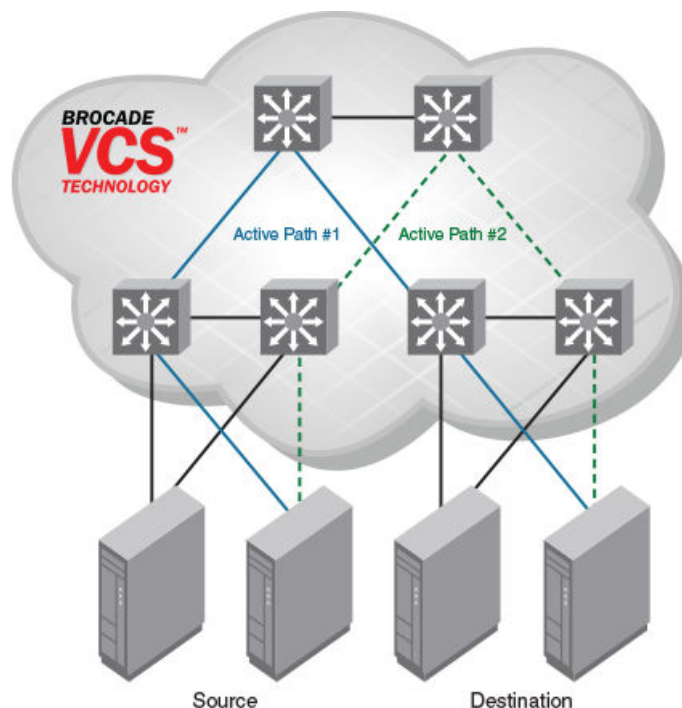
## Automation

Resilience is a foundational attribute of Brocade Fibre Channel storage networks and resilience is also a requirement in modern data centers with clustered applications and demanding compute Service-Level Agreements (SLAs). In developing its VCS Fabric technology, Brocade naturally carried over this core characteristic to its Ethernet fabric design.

In traditional Ethernet networks running Spanning Tree Protocol (STP), only 50 percent of the links are active; the rest (shown as dotted lines in the previous figure) act as backups in case the primary connection fails.

When you connect two or more Brocade VCS Fabric mode-enabled switches they form an Ethernet fabric (provided the two switches have a unique RBridge ID and same VCS ID), as shown in the following figure.

FIGURE 2 Ethernet fabric with multiple paths



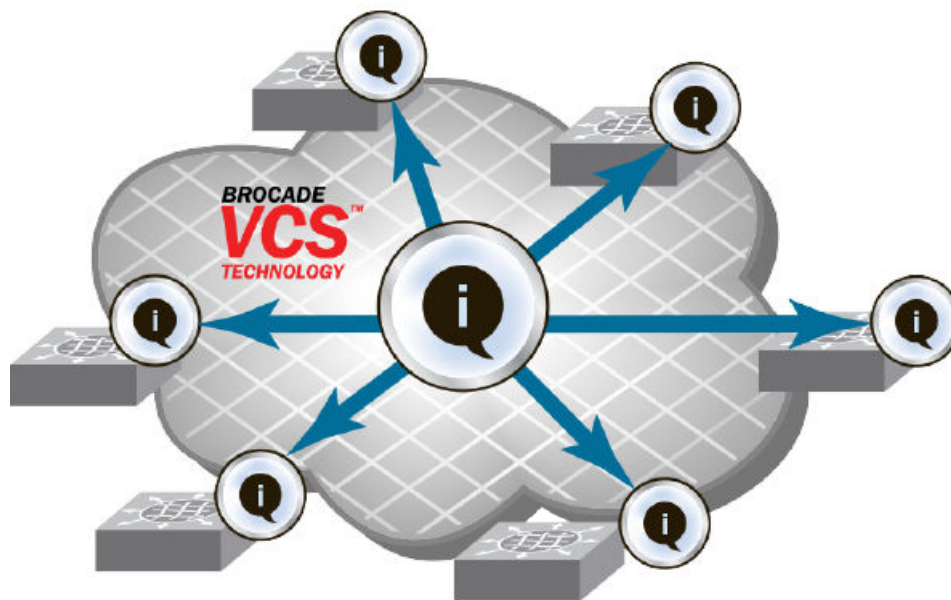
The Ethernet fabric has the following characteristics:

- It is a switched network. The Ethernet fabric utilizes an emerging standard called Transparent Interconnection of Lots of Links (TRILL) as the underlying technology.
- All switches automatically know about each other and all connected physical and logical devices.
- All paths in the fabric are available. Traffic is always distributed across equal-cost paths. As illustrated in the figure, traffic from the source to the destination can travel across two paths.
- Traffic travels across the shortest path.
- If a single link fails, traffic is automatically rerouted to other available paths. In the topology shown in the figure, if one of the links in Active Path #1 goes down, traffic is seamlessly rerouted across Active Path #2.
- STP is not necessary because the Ethernet fabric appears as a single logical switch to connected servers, devices, and the rest of the network.
- Traffic can be switched from one Ethernet fabric path to the other Ethernet fabric path.

## Distributed intelligence

With Brocade VCS Fabric technology, all relevant information is automatically distributed to each member switch to provide unified fabric functionality, as illustrated in the following figure.

FIGURE 3 Distributed intelligence in a Brocade VCS fabric



A Brocade VCS Fabric is designed to be managed as a single "logical chassis," so that each new switch inherits the configuration of the fabric, and the new ports become available immediately. The fabric then appears to the rest of the network as a single switch. This significantly reduces complexity for the management layer, which in turn improves reliability and reduces troubleshooting.

In addition, VCS Fabrics provide a NETCONF application programming interfaces (API), as well as extensions to OpenStack Quantum to orchestrate both physical and logical networking resources as part of virtual machine deployment to support multi-tiered application topologies.

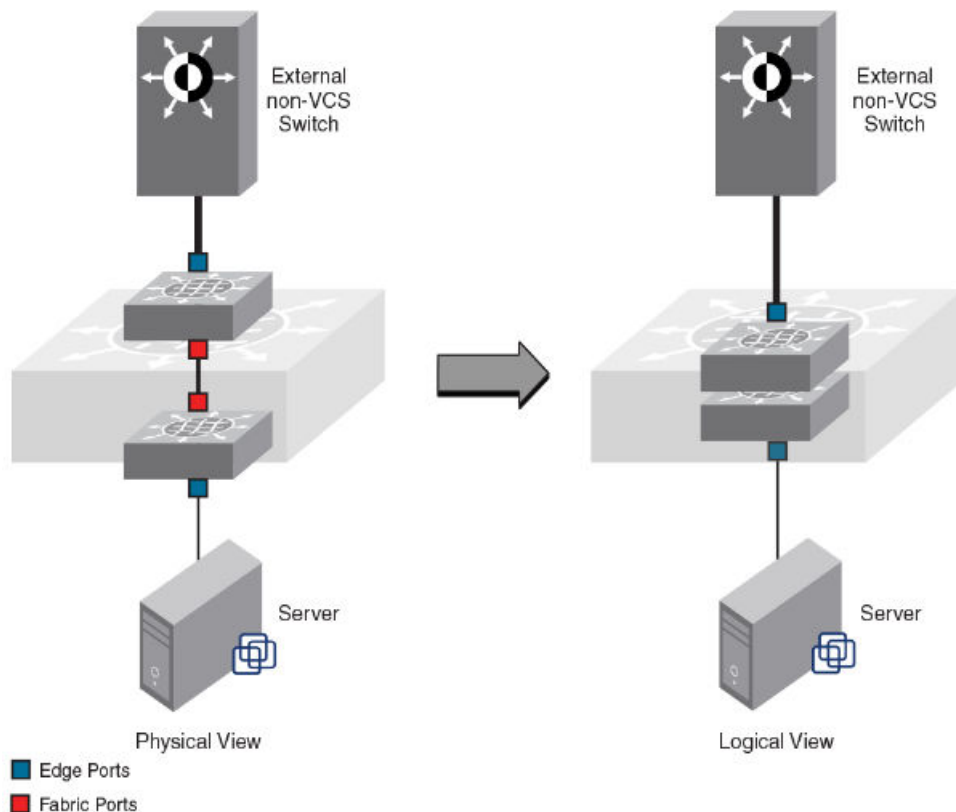
Distributed intelligence has the following characteristics:

- The fabric is self-forming. When two Brocade VCS Fabric mode-enabled switches are connected, the fabric is automatically created and the switches discover the common fabric configuration.
- The fabric is masterless. No single switch stores configuration information or controls fabric operations. Any switch can fail or be removed without causing disruptive fabric downtime or delayed traffic.
- The fabric is aware of all members, devices, and virtual machines (VMs). If the VM moves from one Brocade VCS Fabric port to another Brocade VCS Fabric port in the same fabric, the port-profile is automatically moved to the new port, leveraging Brocade's Automatic Migration of Port Profiles (AMPP) feature.

## Logical chassis

All switches in an Ethernet fabric are managed as if they were a single logical chassis. To the rest of the network, the fabric looks no different from any other Layer 2 switch. The following figure illustrates an Ethernet fabric with two switches. The rest of the network is aware of only the edge ports in the fabric, and is unaware of the connections within the fabric.

FIGURE 4 Logical chassis in Ethernet fabric



Each physical switch in the fabric is managed as if it were a blade in a chassis. When a Brocade VCS Fabric mode-enabled switch is connected to the fabric, it inherits the configuration of the fabric and the new ports become available immediately.

## Ethernet fabric formation

Brocade VCS Fabric protocols are designed to aid the formation of an Ethernet fabric with minimal user configuration. Refer to the “Brocade VCS Fabric formation” section for detailed information about the Ethernet fabric formation process.

All supported switches are shipped with Brocade VCS Fabric mode disabled. Refer to the “Configuring a Brocade VCS Fabric” task for information about disabling and enabling Brocade VCS Fabric mode on your switches.

## Automatic neighbor node discovery

When you connect a switch to a Brocade VCS Fabric mode-enabled switch, the Brocade VCS Fabric mode-enabled switch determines whether the neighbor also has Brocade VCS Fabric mode enabled. If the switch has Brocade VCS Fabric mode enabled and the VCS IDs match, the switch joins the Ethernet fabric.

Refer to the “Configuring a Brocade VCS Fabric” task for information about changing the VCS ID.

## Automatic ISL formation and hardware-based trunking

When a switch joins an Ethernet fabric, ISLs automatically form between directly connected switches within the fabric.



If more than one ISL exists between two switches, then Brocade ISL trunks can form automatically. All ISLs connected to the same neighboring Brocade switch attempt to form a trunk. The trunks are formed only when the ports belong to the same port group. No user intervention is necessary to form these trunks.

Refer to [Configuring fabric interfaces](#) on page 36 for information about enabling and disabling ISLs and trunks.

### Principal RBridge election

The RBridge with the lowest World Wide Name (WWN) in the Ethernet fabric is elected as the principal RBridge.

The role of the principal RBridge is to decide whether a new RBridge joining the fabric conflicts with any of the RBridge IDs already present in the fabric. If a conflict arises, the principal RBridge keeps the joining RBridge segmented.

Refer to [Configuring a Brocade VCS Fabric](#) on page 34 for information about setting the RBridge ID.

## Brocade VCS Fabrics technology use cases

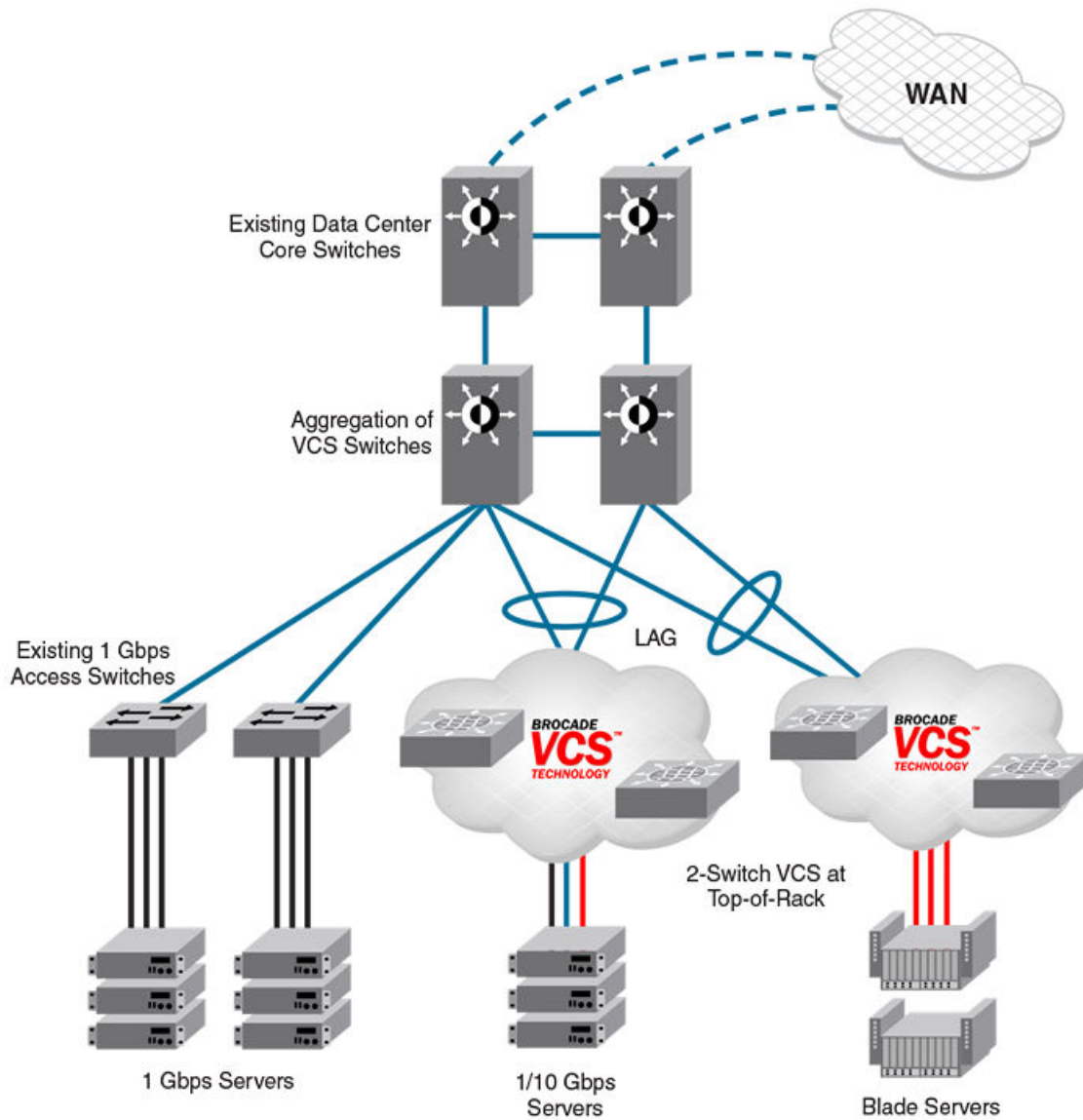
This section describes the following use cases for Brocade VCS Fabrics technology:

- Classic Ethernet
- Large-scale server virtualization
- VCS with FC SAN

### Classic Ethernet access and aggregation use case

Brocade VCS Fabric can be deployed in the same fashion as existing top-of-rack switches, as shown in the following figure. In the right-most two server racks, a two-switch Ethernet fabric replaces the Ethernet switch at the top of each rack.

FIGURE 5 Pair of Brocade VDX switches at the top of each server rack



The servers perceive a single top-of-rack switch, allowing for active/active connections running end-to-end.

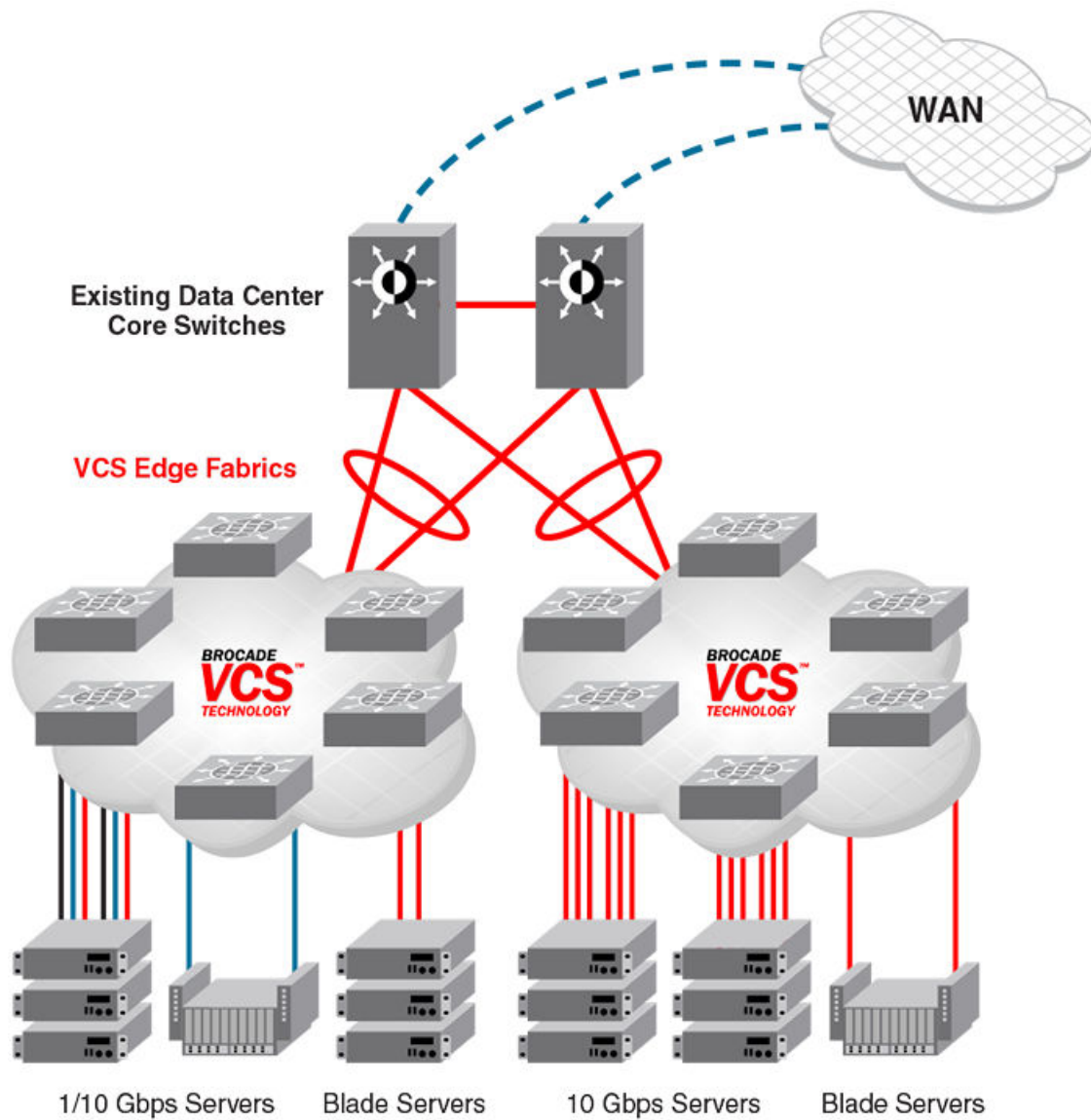
Brocade VCS Fabric technology in this use case provides the following advantages:

- Multiple active-active connections, with increased effective bandwidth
- Preserves existing architecture
- Works with existing core and aggregation networking products
- Co-exists with existing access switches
- Supports 1- and 10-Gbps server connectivity
- Works with server racks or blade servers

## Large-scale server virtualization use case

The following figure shows an example of a logical two-tier architecture with Brocade VCS Fabrics at the edge. Each Brocade VCS Fabric appears as a single virtual switch to the switches outside the fabric, which results in flattening the network.

FIGURE 6 Collapsed, flat Layer 3 networks enabling virtual machine mobility



Brocade VCS Fabric technology in this use case provides the following advantages:

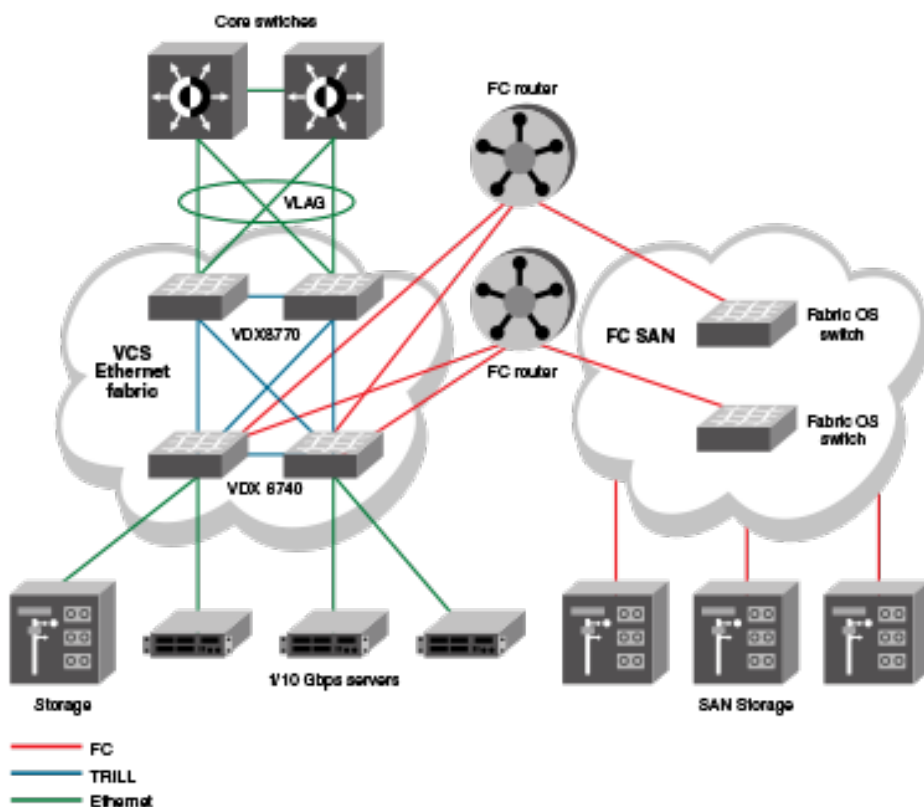
- Optimizes the multipath network (all paths and Layer 3 gateways are active, no single point of failure, and STP is not necessary)
- Increases sphere of virtual machine (VM) mobility

## Brocade VCS Fabric connectivity with Fibre Channel SAN

Using the FlexPort feature on the Brocade VDX 6740 family of hardware, Fibre Channel ports provide support for connecting a Brocade VCS Fabric to a Fibre Channel SAN. Fibre Channel routers provide the connectivity, which provides access to Fibre Channel devices while preserving isolation between the fabrics. Brocade zoning allows you to determine which FCoE devices can access which storage devices on the Fibre Channel SAN.

Brocade VDX 6740 switches can be deployed into your Brocade VCS Fabric as access-level switches, aggregation-level switches, or as a means of attachment to Brocade VCS Fabric aggregation-level switches. Brocade recommends deployment as access-level switches to minimize congestion issues for storage traffic and isolating FCoE traffic from non-FCoE traffic. The following figure shows such a deployment.

FIGURE 7 Brocade VDX 6740 switches deployed as access-level switches



## Topology and scaling

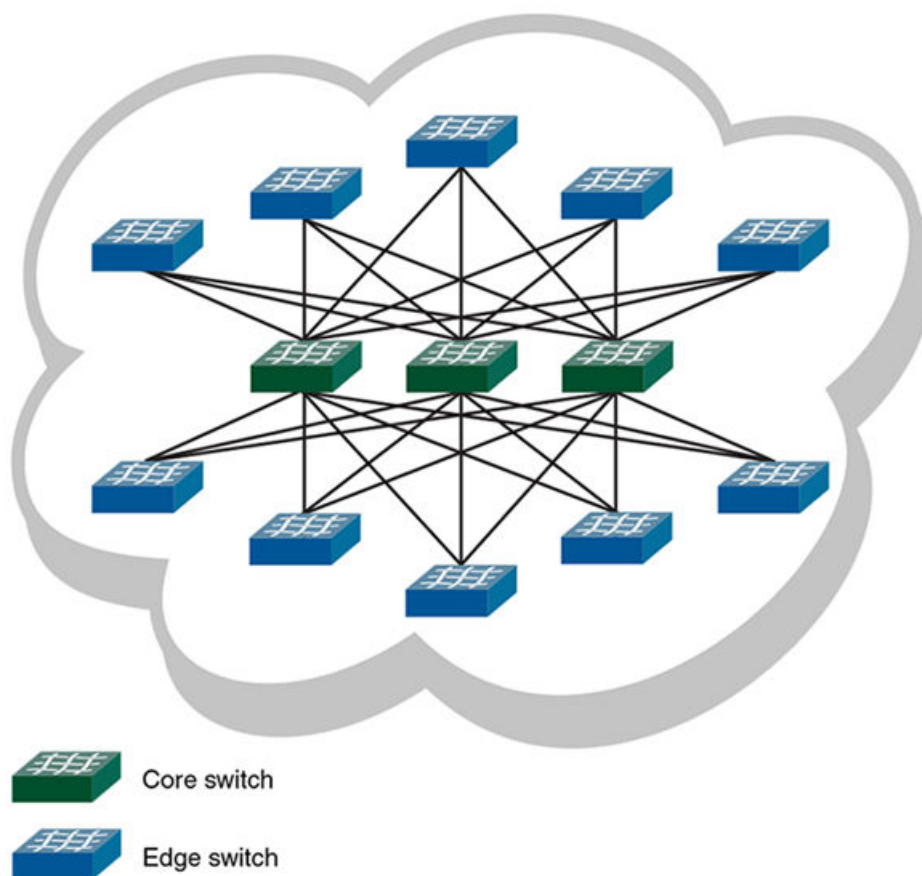
Although you can use any network topology to build a Brocade VCS Fabric, the following topics discuss the scaling, performance, and availability considerations of topologies more commonly found in data centers:

- [Core-edge topology](#) on page 29
- [Ring topology](#) on page 30
- [Full mesh topology](#) on page 30

## Core-edge topology

Core-edge topology devices connect to edge switches, which are connected to each other through core switches. The example shown in the following figure uses three core switches. You could use more or fewer switches in the core, depending on whether you need higher availability and greater throughput, or a more efficient use of links and ports.

FIGURE 8 Core-edge topology



This topology is reliable, fast, and scales well. It is reliable because it has multiple core switches. If a core switch or a link to a core switch fails, an alternate path is available. As you increase the number of core switches, you also increase the number of link or core switch failures your cluster can tolerate.

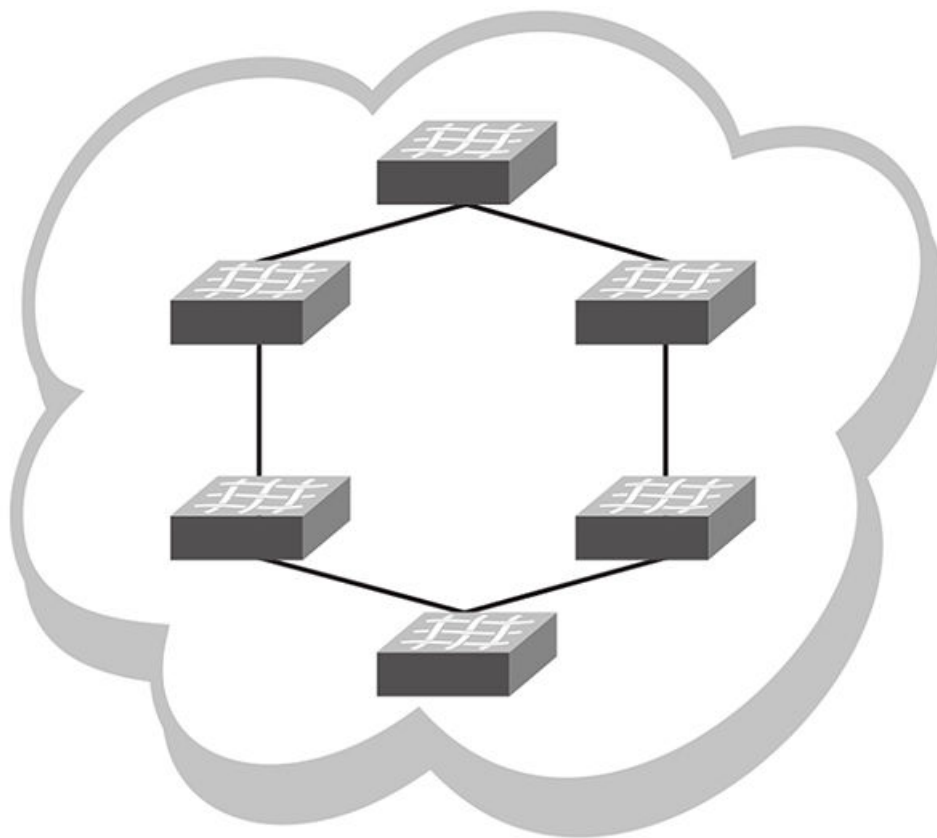
High performance and low latency are ensured because throughput is high and the hop count is low. Throughput is high because multiple core switches share the load. Two hops get you from any edge switch to any other edge switch. If you need greater throughput, simply add another core switch.

Scaling the topology also requires additional core switches and links. However, the number of additional links you need is typically not as great as with, for example, a full mesh topology.

## Ring topology

Ring topology connects each node to exactly two other nodes, forming a single continuous pathway. Data travels from node to node, with each node along the path handling every packet of the data. The following figure shows a ring topology.

FIGURE 9 Ring topology

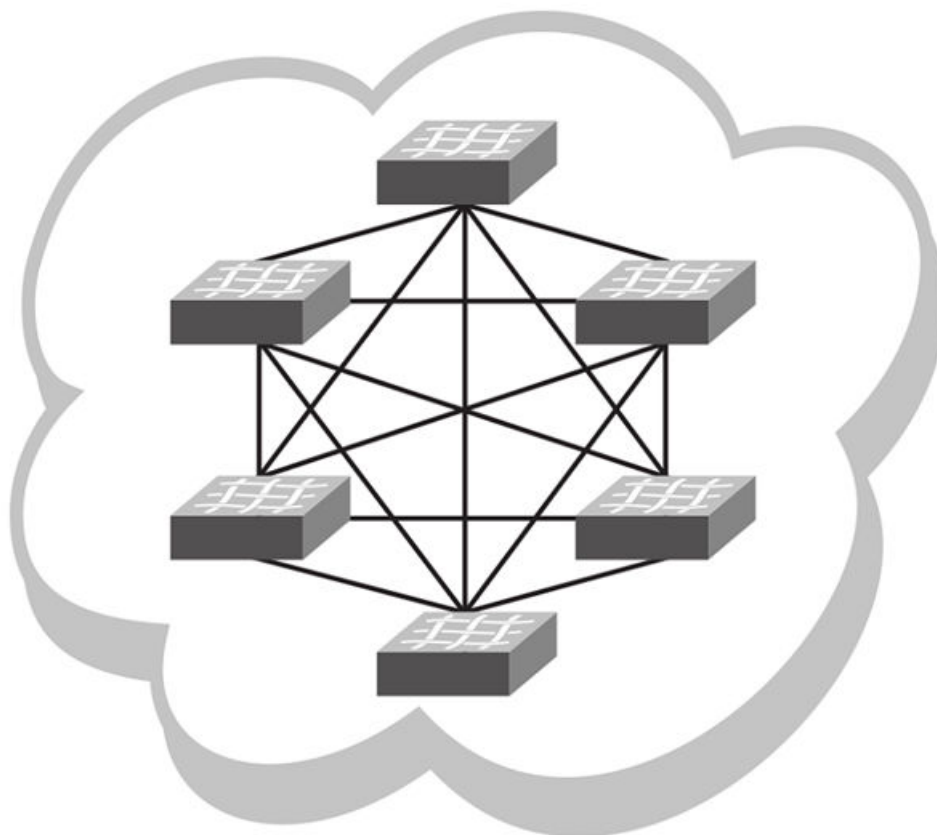


This topology is highly scalable, yet susceptible to failures and traffic congestion. It is highly scalable because of its efficient use of interswitch links and ports; an additional node requires only two ports to connect to the ring. It is susceptible to failures because it provides only one path between any two nodes. Throughput of the fabric is limited by the slowest link or node. Latency can be high because of the potentially high number of hops it takes to communicate between two given switches. This topology is useful where economy of port use is critical, but availability and throughput are less critical.

## Full mesh topology

Full mesh topology connects each node to all other cluster nodes, as shown in the following figure.

FIGURE 10 Full mesh topology



This topology is highly reliable and fast, but it does not scale well. It is reliable because it provides many paths through the fabric in case of cable or node failure. It is fast with low latency because you can get to any node in the fabric in just one hop. It does not scale well because each additional node increases the number of fabric links and switch ports exponentially. This topology is suitable for smaller fabrics only.

## Fabric overview

The Brocade VCS Fabric Ethernet fabric is defined as a group of switches that exchange information between each other to implement distributed intelligence. The Brocade Ethernet fabric uses Transparent Interconnection of Lots of Links (TRILL) protocol, designed for the sole purpose of scaling Ethernet networks by allowing a set of devices, called routing bridges (RBridges), to connect with each other.

A link state dynamic routing protocol, rather than Spanning Tree Protocol, determines how the traffic is forwarded between the interconnected RBridges. Link state routing in Brocade VCS Fabric-based TRILL networks is performed using Fabric Shortest Path First (FSPF) protocol.

TRILL enables Layer 2 networks to behave like routed Layer 3/IP networks. TRILL also defines native support for forwarding both unicast and multicast traffic, and therefore unifies support for both of these different classes of applications over a single transport.

## Brocade VCS Fabric formation

Brocade VCS Fabric technology uses RBridge identifiers (IDs) to discover fabric creation problems, such as duplicate IDs. The RBridge ID of a cluster unit is equal to the domain ID of an FC switch. RBridge ID assignment is implemented by leveraging the domain ID assignment protocols in the FC SANs. Request for Domain ID (RDI) and Domain ID Assignment (DIA) protocols ensure that a single switch (the principal switch) is centrally allocating the domain IDs for every RBridge in the fabric and detecting any domain ID conflicts in the fabric. In case of conflict, the conflicting node is segmented from the fabric. You must take action to resolve the conflict

### NOTE

Network OS 5.0.1 and later support a maximum of 48 RBridges in a single Brocade VCS Fabric, depending on the hardware mix. However, Brocade recommends using only 24 RBridges per fabric.

The following sequence of events describes the Brocade VCS Fabric formation process:

- Each Brocade VCS Fabric is identified by a VCS ID.
- All Brocade VCS Fabric-capable switches are configured with a factory default VCS ID of 1.
- The switch software searches for the value for the "VCS enable" attribute setting and verifies it is set to "enabled".
- Assuming the switch is Brocade VCS Fabric-enabled, the switch software invokes a series of protocols:
  - Brocade Link Discovery Protocol (BLDP) attempts to discover if a Brocade VCS Fabric-capable switch is connected to any of the edge ports. Refer to [Neighbor discovery](#) on page 33 for more information.
  - BLDP attempts to merge the adjacent Brocade switch into the Brocade VCS Fabric environment at the link level.
- A series of FC fabric formation protocols (RDI, DIA, and FSPF) are initiated once a link level relationship has been established between two neighbor switches. Refer to [Fabric formation](#) on page 34 for more information.
- The "Merge and Join" protocol invokes a merge of switch configuration between the cluster units once the fabric has successfully formed.

## How RBridges work

RBridges find each other by exchanging FSPF Hello frames. Like all TRILL IS-IS frames, Hello frames are transparently forwarded by RBridges and are processed by RBridge Inter-Switch Link (ISL) ports. Using the information exchanged in the Hello frames, the RBridges on each link elect the designated RBridge for that link.

The RBridge link state includes information such as VLAN connectivity, multicast listeners, and multicast router attachment, claimed nicknames, and supported ingress-to-egress options. The designated RBridge specifies the appointed forwarder for each VLAN on the link (which could be itself) and the designated VLAN for inter-RBridge communication. The appointed forwarder handles native frames to and from that link in that VLAN.

The Ingress RBridge function encapsulates frames from the link into a TRILL data frame. The Egress RBridge function decapsulates native frames destined for the link from the TRILL data frames. TRILL data frames with known unicast destinations are forwarded by RBridge next hop. Multi-destination frames (broadcast, unknown unicast, and multicast) are forwarded on a tree rooted at the multicast root RBridge.

- Unicast forwarding is handled by combining domain routing generated by FSPF and MAC-to-RBridge learning generated by MAC learning and a distributed MAC database.
- Multicast forwarding usually uses one tree that is rooted at the RBridge with the lowest RBridge ID. However, there are several rules for Multicast root tree selection. It is not always the lowest RBridge ID.

If a duplicated RBridge ID is found while the links are still coming up, the links are segmented. Both sides recognize the error and segment the link. If the RBridge ID overlap cannot be found at ISL link bringup time (in the case where a new switch is brought from an offline state into the fabric) it will be found during the fabric build and the conflicting switch is isolated.



An RBridge requests a specific RBridge ID from the coordinator switch. If the coordinator switch detects that this RBridge ID is already used, it returns the next unused RBridge ID. The requesting RBridge is not allowed to take another RBridge ID and it segments itself from the fabric. In this case, you cannot boot the ISLs. The ISLs have to be explicitly disabled and then enabled again in order for the RBridge with the overlapping RBridge ID to be removed.

## Neighbor discovery

Brocade VCS Fabric-capable neighbor discovery involves the following steps:

- Discover whether the neighbor is a Brocade switch.
- Discover whether the Brocade neighbor switch is Brocade VCS Fabric-capable.

Only Brocade VCS Fabric-capable switches with the same VCS ID can form a virtual cluster switch. The default settings for Brocade Network OS switches are Brocade VCS Fabric capable and a VCS ID of "1."

## Brocade trunks

Network OS 4.0.0 and later supports Brocade trunks (hardware-based link aggregation groups, or LAGs). These LAGs are dynamically formed between two adjacent switches. The trunk formation is controlled by the same Fibre Channel Trunking protocol that controls the trunk formation on FC switches. As such, it does not require user intervention or configuration except enabling or disabling, which instructs the switch software to form a trunk at the global level or not. All ISL ports connected to the same neighbor Brocade switch will attempt to form a trunk. Refer to [Enabling a fabric trunk](#) on page 37 for instructions.

Port groups have been established on supported standalone switches and on line cards in chassis systems for trunking. For a successful trunk formation, all ports on the local switch must be part of the same port group and must be configured at the same speed. Following are the number of ports allowed per trunk from port groups in supported platforms. For details on how port groups are arranged on these platforms, refer to the switch or chassis system Hardware Reference Manual.

- VDX 8770 switches - up to six port groups of eight ports each per blade (1, 10, or 40 GbE)
- VDX 6740 switches - up to 16 ports per trunk

### NOTE

If connections are made to 16 different switches, only eight ports will be trunk ports while the other eight ports will be normal ISL ports.

- VDX 6940-36Q switches - up to three ports per trunk
- VDX 2741 and VDX 2746 - up to 16 ports per trunk
- 48x10 GbE line card - up to eight ports per trunk
- 48x10G-T line card - up to 16 ports per trunk
- 12x40 GbE line card - up to two 40-GbE ports are allowed per trunk, and these ports must be configured in breakout mode
- 27x40 GbE line card - up to two 40-GbE ports are allowed per trunk, and these ports must be configured in breakout mode. Note that breakout mode is only allowed on the first two ports in port groups that are configured in Performance operating mode. Refer to the *Brocade 8770 Hardware Reference Manual* for more information on line card operating modes.

The following additional rules apply to Brocade trunks:

- On Brocade VDX 6740 switches, low-volume traffic below certain thresholds may not be evenly distributed on all links. This threshold can be as low as 64 K.
- The trunk is turned on by default.
- Trunks are not supported between the Brocade 8000 and the Brocade VDX 8770.

## Fabric formation

Brocade VCS Fabric technology leverages proven FC Fabric protocols to build a TRILL fabric. The main functions of the fabric formation protocols are as follows:

- Assign the Brocade VCS Fabric-wide unique RBridge IDs (Domain ID Assignment).
- Create the network topology database using link state routing protocol (Fabric Shortest Path First, or FSPF). FSPF calculates the shortest path routes to a destination RBridge.
- Distribute fabric multicast traffic.

## Principal switch selection

Every Brocade VCS Fabric-enabled switch, upon boot-up and after the Fabric port formation, declares itself to be a principal switch and advertises this intent on all fabric ports. The intent includes a priority and its switch WWN. If all switches boot up at the same time, the default priority is the same and all switches will compare their mutual intents. The switch with the lowest Switch WWN becomes the principal switch. The WWN is an industry-standard burnt-in switch identifier, similar to the Bridge-MAC except it is 8 bytes. The role of the principal switch is to decide whether a new RBridge joining the fabric conflicts with any of the RBridge IDs already present in the fabric. At the end of the principal switch selection process, all the switches in the cluster have formed a tree with the principal switch at the root.

### NOTE

Brocade VDX Data Center switches are shipped with factory-programmed world wide names (WWNs) that are unique.

### NOTE

In a logical chassis cluster, you can select the principal node by using the command line interface. For more information, refer to [Selecting a principal node for the cluster](#) on page 79.

## RBridge ID allocation

RBridge ID assignment is implemented by leveraging proven Domain ID assignment protocols from FC SANs. Request for Domain ID (RDI) and Domain ID Assignment (DIA) protocols ensure that a single switch (the principal switch) centrally allocates the domain IDs for every RBridge in the fabric and detects and resolves any domain ID collisions in the fabric. A Brocade VCS Fabric supports up to 48 RBridge IDs. RBridge IDs can range from 1 through 239.

Only the principal switch can allocate RBridge IDs (domain IDs) for all other switches in the fabric. The principal switch starts the allocation process by allocating an RBridge ID for itself (using the ID value supplied by the user), and initiates the DIA messages on all ports.

Other switches, which are now in subordinate mode, upon receiving the DIA frames respond with an RDI message towards the principal switch. The process continues until all the switches in the fabric have been allocated a unique ID.

## Fabric routing protocol

After a RBridge ID is assigned to a switch, the Fabric Shortest Path First (FSPF) link state routing protocol begins to form adjacencies and collects topology and inter-connectivity information with its neighbors. Brocade VCS Fabric uses FSPF to calculate and elect a loop-free multicast tree rooted at the multicast root RBridge. The multicast tree is calculated after the unicast routes are computed.

## Configuring a Brocade VCS Fabric

Refer to the following tables for commands and examples used in configuring a Brocade VCS Fabric. For command details, refer to the *Network OS Command Reference*.

The following table lists command examples for enabling Brocade VCS logical chassis cluster mode:

**TABLE 5** Command examples for enabling logical chassis cluster mode

Command	Command Behavior
<code>switch# vcs logical-chassis enable</code>	The VCS ID becomes the default value of 1, the RBridge ID is not changed, and Brocade VCS logical chassis cluster mode is enabled.
<code>switch# vcs vcsid 22 rbridge-id 15 logical-chassis enable</code>	The VCS ID is changed to 22, the RBridge ID is changed to 15, and Brocade VCS logical chassis cluster mode is enabled. RBridge IDs range from 1 through 239.
<code>switch# vcs vcsid 11 logical-chassis enable</code>	The VCS ID is changed to 11, the RBridge ID is not changed, and Brocade VCS logical chassis cluster mode is enabled.
<code>switch# vcs rbridge-id 6 logical-chassis enable</code>	The VCS ID becomes the default value of 1, the RBridge ID is changed to 6, and Brocade VCS logical chassis cluster mode is enabled.

The following table lists command examples for enabling Brocade VCS fabric cluster mode:

**TABLE 6** Command examples for enabling fabric cluster mode

Command	Command Behavior
<code>switch# vcs vcsid 55 rbridge-id 19 enable</code>	The VCS ID is changed to 55, the RBridge ID is changed to 19, and Brocade VCS fabric cluster mode is enabled.
<code>switch# vcs vcsid 73 enable</code>	The VCS ID is changed to the value of 73, the RBridge ID is not changed, and Brocade VCS fabric cluster mode is enabled.
<code>switch# vcs rbridge-id 10 enable</code>	The VCS ID becomes the default value 1, the RBridge ID is changed to 10, and Brocade VCS fabric cluster mode is enabled.

The following table lists command examples for switches that are already in either fabric cluster mode or logical chassis cluster mode.

**TABLE 7** Command examples for when one of the VCS modes is already enabled:

Command	Command Behavior
<code>switch# vcs vcsid 44 rbridge-id 22</code>	The VCS ID is changed to 44 and the RBridge ID is changed to 22.
<code>switch# vcs vcsid 34</code>	The VCS ID is changed to 34.

## Adding a new switch into a fabric

There are two methods to add a new switch into a fabric: The auto-fabric method and the manual method. For the auto-fabric method, refer to the "Auto Fabric" section of this manual.

To add a new switch into the Brocade VCS fabric manually, complete the following configuration steps.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **vcs rbridge-id rbridge-id enable** command.

The switch remembers its RBridge ID once it has been assigned. The **vcs rbridge-id rbridge-id enable** command also sets the insistent RBridge ID property on the switch.

3. Reboot the system.

After the required reboot the switch participates in the RBridge ID allocation protocol, which insists that the same value that was manually configured prior to reboot be allocated after reboot.

The switch is not allowed into the fabric if there is a conflict; for example, if another switch with the same ID exists and is operational in the fabric. You have the opportunity to select a new RBridge ID by using the same CLI.

Once an ID has been assigned by the fabric protocol, these IDs are then numerically equated to RBridge IDs and are treated as such after that.

Use the **vcs** command to configure the Brocade VCS Fabric parameters, VCS ID, and the switch RBridge ID, and to enable Brocade VCS Fabric mode (also called *VCS mode*).

VCS mode encompasses two mode types:

- *Fabric cluster mode* — The data path for nodes is distributed, but the configuration path is not distributed. Each node keeps its configuration database independently.
- *Logical chassis cluster mode* — Both the data and configuration paths are distributed. The entire cluster can be configured from the principal node. Logical chassis cluster mode requires Network OS 4.0 or later.

The generic term *VCS mode* in this manual applies to both fabric cluster mode and logical chassis cluster mode unless otherwise stated.

You can set the Brocade VCS Fabric parameters and enable VCS mode at the same time, or you can enable VCS mode and then perform the ID assignments separately. Refer to [Configuring a Brocade VCS Fabric](#) on page 34 for details.

After configuring the Brocade VCS Fabric parameters, the switch applies the changes and reboots.

The switch disable is not saved across a reboot, so if the switch was disabled prior to the reboot, the switch returns to the enabled state when it finishes the boot cycle.

## Configuring fabric interfaces

A physical interface in a virtual switch cluster can either be an edge port or a fabric port, but not both. Similar to a switch-port configuration on a physical interface, you can also change a fabric-port configuration on its physical interface by using the **fabric ISL enable** and **fabric trunk enable** commands, described below.

### Enabling a fabric ISL

The **fabric isl enable** command controls whether an ISL should be formed between two cluster members. With the default setting of ISL discovery to **auto** and the ISL formation mode to **enable**, an ISL automatically forms between two cluster switches.

Performing a **fabric isl enable** command on an operational ISL has no effect. However, performing a **no fabric isl enable** command on an interface toggles its link status and subsequently disables ISL formation. In addition, the **no fabric isl enable** command triggers the switch

to inform its neighbor that the local interface is ISL disabled. Upon receiving such information, a neighbor switch stops its ISL formation activity regardless of its current interface state.

#### NOTE

After you repair any segmented or disabled ISL ports, toggle the fabric ISL in order to propagate the changes.

#### NOTE

A **shutdown** command on an operating ISL interface not only brings down the physical link but also its FSPF adjacency. The main difference between a **shutdown** command and a **no fabric isl enable** command is that the link stays up after a **no fabric isl enable**, while the link stays down after a shutdown.

#### NOTE

Upon a fabric reconvergence that due to a topology change involving the ECMP fabric-isl path, there may be sub-second flooding of known unicast traffic.

## Disabling a fabric ISL

The **no fabric isl enable** command takes this interface out of the trunk group if this interface happens to be currently part of the trunk. If you know and would like to fix the edge and fabric port assignments on a switch, then this command allows you to completely turn off ISL formation logic and shorten any link bring-up delays on edge ports.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **no fabric isl enable** command.

## Enabling a fabric trunk

#### NOTE

Trunks are not supported between the Brocade 8000 and the Brocade VDX 8770.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **fabric trunk enable** command.

## Disabling a fabric trunk

Fabric trunking is enabled by default. Enter the **no fabric trunk enable** command to revert the ISL back to a standalone adjacency between two Brocade VCS Fabric switch.

## Configuring broadcast, unknown unicast, and multicast forwarding

All switches in a Brocade VCS Fabric cluster share a single multicast tree rooted at the RBridge with the lowest RBridge ID (domain ID). All broadcast, unknown unicast, and multicast traffic between two edge RBridges is forwarded on this multicast tree inside the Brocade VCS Fabric. The multicast tree includes all RBridges in the Brocade VCS Fabric.

### Multicast distribution tree-root selection

Network OS supports the following distribution tree behaviors.

- The root of the distribution tree is the switch with the lowest RBridge ID. The automated selection process does not require any user intervention.
- Each switch in the cluster optionally carries a multicast root priority. This priority setting overrides the automatically-selected multicast root. In deployments where a multicast root is required to be a specific switch that does not have the lowest RBridge

ID, then the priority setting on that switch can override the root selection. If there are two switches with the same priority, then the switch with the lower RBridge ID prevails.

- A back-up multicast root is pre-selected, which is the switch with the next lowest RBridge ID. The back-up multicast root is automatically selected by all switches should the current multicast root fail.

## Configuring priorities

As stated above, the root of the tree is auto-selected as the switch with the lowest RBridge ID. For example, if you had a cluster with RBridge IDs 5, 6, 7, and 8, then 5 would be the root. If you then added RBridge ID 1 to this fabric, the tree would be re-calculated with 1 as the root.

In order to avoid this behavior, you can set a priority (default is 1). The highest priority overrides the lowest RBridge ID and becomes the root.

For example, to build a fabric with RBridge ID 7 or 8 as the root, set their priority to something higher than 1 (priority values are 1 through 255). If there is a tie in priority, the lower RBridge is still chosen. If RBridge ID 7 and 8 are both set to priority 1, 7 becomes the root.

## Changing the priority

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **fabric route mcast rbridge-id** command.

Here is an example of changing an RBridge multicast priority:

```
switch(config)# fabric route mcast rbridge-id 12 priority 10
```

## Displaying the running configuration

The **show running-config fabric route mcast** command allows you to display fabric route multicast configuration information. The configuration currently effective on the switch is referred to as the running configuration. Any configuration change you make while the switch is online is made to the running configuration. The running configuration is nonpersistent.

### NOTE

To save configuration changes, you must save the running-config file to a file, or you can apply the changes by copying the running configuration to the startup configuration.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the show running-config fabric route mcast command.

```
switch# show running-config fabric route mcast priority
fabric route mcast rbridge-id 12 priority 10
```

## Configuring VCS virtual IP addresses

A virtual IP address is assigned for each VCS cluster. This virtual IP address is tied to the principal switch in the cluster. The management interface of the principal switch can be accessed by means of this virtual IP address. Because the virtual IP address is a property of the fabric cluster and logical chassis cluster, in the event that the principal switch goes down, the next principal switch is assigned this address.

Virtual IP address can be configured by means of the **vcs virtual ip address** command:

```
switch(config)# vcs virtual ip address 10.0.0.23/24
```

This command can be used in logical chassis cluster and fabric cluster modes only. When the virtual IP address is configured for the first time, the current principal switch in the cluster is assigned this IP address.

Virtual IP configuration is global in nature. All the nodes in the cluster are configured with the same virtual IP address, but address is bound to the current principal switch only. Make sure that the assigned virtual IP address is not a duplicate of an address assigned to any other management port in the cluster or network.

Brocade recommends that you use a /32 address in the same subnet as the IP address of the management interface. For example, if you are using inband management via rbridge interface ve 100 with the ip address 192.168.100.10/24, set your vcs virtual ip address as a /32 address in this subnet by using the command **vcs virtual ip address 192.168.100.1/32**. To display the currently configured virtual IP address, use the **show vcs virtual ip** command:

```
switch# show vcs virtual ip

Virtual IP           : 10.21.87.2/20
Associated rbridge-id : 2
```

To remove the currently configured virtual IP address, use the **no vcs virtual ip address** command.

```
switch(config)# no vcs virtual ip address
switch# show running-config vcs virtual ip address
% No entries found.
```

#### NOTE

You should not use the **no vcs virtual ip address** command when logged onto the switch through the virtual IP address. Use the management port IP address of the principal switch, or the serial console connection of the principal switch.

If you wish to rebind this virtual IP address to this management interface, remove the currently configured virtual IP address and reconfigure it. This situation can arise when the virtual IP address is not bound to management interface of the principal switch as a result of duplicate address detection.

A separate gateway cannot be configured for virtual IP address. The default gateway is the same as the gateway address for the management port of the same switch.

## Virtual IP address configuration scenarios

Virtual IP address may be assigned to a switch whenever it is the principal switch in the cluster. The configuration scenarios that may occur are described below.

**TABLE 8** Virtual IP address configuration scenarios

Scenario	Description
First time cluster formation	When the cluster is first being formed, and if the virtual IP address is already configured, the principal switch is assigned the Virtual IP address. If no Virtual IP configuration exists, then the principal switch can be access using the management port IP address.
Virtual IP configuration	When you configure the virtual IP address for a cluster the first time, the address is bound to the management interface of the principal switch.
Principal switch failover	If the principal switch becomes a secondary switch while the virtual IP address is assigned to its management interface, then the virtual IP address is reassigned to the new principal switch.
Principal switch goes down	When the principal switch in the cluster goes down, the virtual IP address is released from its management interface. The virtual IP address will be assigned to the next switch that becomes the principal switch.
Principal switch chassis is disabled	When the <b>chassis disable</b> command is executed on the principal switch, the virtual IP address is released from its management interface. The virtual IP address will be assigned to the next switch that becomes the principal switch.

**TABLE 8** Virtual IP address configuration scenarios (continued)

Scenario	Description
Virtual IP removal	If you remove the virtual IP address from the configuration, then the address is unbound from management interface of the principal switch. In this case, the principal switch can still be accessed by using the management port's IP address.
Trivial merge	In the event that two clusters merge together, the global configuration of the smaller cluster (Cluster A) is overwritten by the larger cluster (Cluster B). During this time, the virtual IP address is unbound from the principal switch of Cluster A. The virtual IP address of Cluster B can now be used to access the principal of new merged cluster. If the virtual IP address of Cluster B is not configured, there will not be a virtual IP address in the merged cluster.
Cluster reboot	When the cluster reboots, the virtual IP address is persistent and is bound to the new principal switch.
Cluster Islanding	If the ISL link goes down between two or more clusters that are forming, the principal switch in the original cluster retains the virtual IP address. The new principal switch in the second cluster will perform a check to confirm that the virtual IP address is not in use. If it is in use, then the address is not assigned to the switch and an error is logged in RASLog.
Virtual MAC address	Virtual MAC address are not supported by virtual IP addresses.
Management port primary IPv4 address	For a virtual IP address to work correctly, the management port's IPv4 address should be assigned and functional.

## Configuring fabric ECMP load balancing

Traffic towards ECMP paths are load-balanced using the following eight fields as the Key; VlanID, MAC DA/SA, L3\_ULP, L3 DA/SA, L4 Dst/Src. For some pattern of streams, most of the traffic falls into one ECMP path, and rest of the ECMP paths are underutilized. This results in loss of data traffic, even though more ECMP paths are available to offload the traffic. You can configure the ECMP path selection method within the fabric by using the **fabric ecmp load-balance** command in RBridge ID configuration mode. The operands for this command are listed and described in the following table.

**TABLE 9** ECMP load-balancing operands

Operand	Description
<b>dst-mac-vid</b>	Destination MAC address and VID-based load balancing
<b>src-dst-ip</b>	Source and Destination IP address-based load balancing
<b>src-dst-ip-mac-vid</b>	Source and Destination IP and MAC address and VID-based load balancing
<b>src-dst-ip-mac-vid-port</b>	Source and Destination IP, MAC address, VID and TCP/UDP port based load balancing
<b>src-dst-ip-port</b>	Source and Destination IP and TCP/UDP port-based load balancing
<b>src-dst-mac-vid</b>	Source and Destination MAC address and VID-based load balancing
<b>src-mac-vid</b>	Source MAC address and VID-based load balancing

Additionally, you can choose to swap adjacent bits of the hash key using the **fabric ecmp load-balance-hash-swap** command. This is useful in cases where a choice of any of the hash key combinations causes the distribution of traffic to not be uniform.

The **fabric ecmp load-balance-hash-swap** command is used to configure the swapping of the input fields before feeding them to the hash function. The integer is interpreted as a bitwise control of the 212-bit key. Each bit controls whether the two adjacent bits of the key are to be swapped. This 32-bit control value is written to all four hash swap control registers. This value is replicated in 32-bit block to form a 106-bit value. A value of 0x0 does not swap any input fields while a value of 0xffffffff swaps all 106 input bit-pairs.



**NOTE**

The **fabric ecmp load-balance-hash-swap** command is supported on the Brocade VDX 8770.

To configure the ECMP load-balancing feature, perform the following steps in global configuration mode.

1. Enter RBridge ID configuration mode.

```
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)#
```

2. Execute the **fabric ecmp load-balance** command for the stream you want to favor.

This example uses the Destination MAC address and VID-based load balancing flavor.

```
switch(config-rbridge-id-2)# fabric ecmp load-balance dst-mac-vid
```

3. Optional: Use the **fabric ecmp load-balance-hash-swap** command to swap the input fields before feeding them to the hash function.

```
switch(config-rbridge-id-2)# fabric ecmp load-balance-hash-swap 0x4
```

4. Use the **show fabric ecmp load-balance** command to display the current configuration of hash field selection and hash swap.

```
switch# show fabric ecmp load-balance
Fabric Ecmp Load Balance Information
-----
Rbridge-Id          : 2
Ecmp-Load-Balance Flavor : Destination MAC address and VID based load balancing
Ecmp-Load-Balance HashSwap : 0x4
```



# Basic Switch Management

---

• Switch management overview.....	43
• Ethernet management interfaces.....	55
• Stateless IPv6 autoconfiguration.....	56
• Switch attributes.....	56
• Switch types.....	56
• Operational modes.....	57
• Modular platform basics.....	61
• Supported interface modes.....	63
• Slot numbering and configuration.....	64
• Connecting to a switch.....	64
• Using the management VRF.....	68
• Configuring and managing switches.....	68
• Configuring policy-based resource management and hardware profiles.....	91
• Auto Fabric.....	99
• Using maintenance mode for graceful traffic diversion (VCS Fabrics only).....	101
• Tunable SFP+ optics.....	106

## Switch management overview

In addition to connecting to Brocade switches, an understanding of switch types, attributes, and operational modes is essential to the successful installation and management of networks. This chapter introduces the operational modes, command modes and submodes, and other switch-related activities (such as troubleshooting and managing high-availability scenarios), providing an essential reference for everyday management operations.

## Connecting to a switch

You can connect to your switch through a console session on the serial port, or through a Telnet or Secure Shell (SSH) connection to the management port or the inband port belonging to either "mgmt-vrf" or "default-vrf". You can use any account login present in the local switch database or on a configured authentication, authorization, and accounting (AAA) server for authentication. For initial setup procedures, use the pre-configured administrative account that is part of the default switch configuration.

The switch must be physically connected to the network. If the switch network interface is not configured or the switch has been disconnected from the network, use a console session on the serial port.

- Refer to the *Brocade VDX Hardware Reference* manuals for information on connecting through the serial port.
- Refer to [Configuring Ethernet management interfaces](#) on page 68 for details on configuring the network interface.

## Telnet and SSH

Telnet and Secure Shell (SSH) are mechanisms for allowing secure access to management functions on a remote networking device. SSH provides a function similar to Telnet, but unlike Telnet, which offers no security, SSH provides a secure, encrypted connection to the device.

SSH and Telnet support is available in privileged EXEC mode on all Brocade VDX platforms. Both IPv4 and IPv6 addresses are supported.

Telnet and SSH services are enabled by default on the switch. When the Telnet server or SSH server is disabled, access to the switch is not allowed for inbound Telnet or SSH connections, thereby restricting remote access to the switch.

Network OS supports up to 32 CLI sessions on a switch.

In configuration mode, the CLI can be used to disable Telnet or SSH service on the switch. Doing so will terminate existing inbound Telnet or SSH connections and block any new inbound Telnet or SSH connections to the switch. Additional inbound Telnet or SSH connections will not be allowed until the Telnet server or SSH server is re-enabled. If you have admin privileges, you can re-enable inbound Telnet or SSH connections from configuration mode.

If you are in logical chassis cluster mode (refer to [Operational modes](#) on page 57), the command for enabling or disabling Telnet or SSH services is not distributed across the cluster. The RBridge ID of the node should be used to configure the service on individual nodes.

In operational mode, you can use the **show** command to display whether Telnet or SSH is enabled or disabled on the switch.

#### NOTE

Telnet alone is not supported on the Brocade VDX 2746. Telnet port 23 is denied by default.

## SSH server key exchange and authentication

The Secure Sockets Handling (SSH) protocol allows users to authenticate using public and private key pairs instead of passwords. In password-based authentication, the user must enter a password for authentication purposes. In public-key authentication, the user should have a private key in the local machine and a public key in the remote machine. The user should be logged in to the local machine to be authenticated. If a passphrase is provided while generating the public and private key pair, it must be entered to decrypt the private key while getting authenticated.

SSH key-exchange specifies the method used for generating the one-time session keys for encryption and authentication with the SSH server. A user is allowed to configure the SSH server key-exchange method to DH Group 14. When the SSH server key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client is also configured to DH Group 14.

The following steps briefly describe public-key authentication:

1. The user generates a pair of encryption keys in a local machine using the **ssh-keygen** command, along with the public and private key, as shown below. Messages encrypted with the private key can only be decrypted by the public key, and vice-versa.

```
switch# ssh-keygen -t rsa
generates RSA public and private keypair
switch# ssh-keygen -t dsa
generates DSA public and private keypair
```

2. The user keeps the private key on the local machine, and uploads the public key to the switch.
3. When attempting to log in to the remote host, the user receives an encrypted message from the remote host containing the public key. After the message is decrypted in the local host by means of the private key, the user is authenticated and granted access.

The **ssh-keygen** command is not distributed across the cluster. The RBridge ID of the node should be used to configure service on individual nodes.

## Feature support for Telnet

The following features are not supported with Telnet:

- Displaying Telnet sessions
- Terminating hung Telnet sessions

## Feature support for SSH

SSHv2 is the supported version of SSH, but not all features typically available with SSHv2 are supported on the Brocade VDX family of switches.

The following encryption algorithms are supported:

- **3des** Triple-DES (default)
- **aes256-cbc** : AES in CBC mode with 256-bit key
- **aes192-cbc** : AES in CBC mode with 192-bit key
- **aes128-cbc** : AES in CBC mode with 128-bit key

The following Hash-based Message Authentication Code (HMAC) message authentication algorithms are supported:

- **hmac-md5** : MD5 encryption algorithm with 128-bit key (default).
- **hmac-md5-96** : MD5 encryption algorithm with 96-bit key.
- **hmac-sha1** : SHA1 encryption algorithm with 160-bit key.
- **hmac-sha1-96**: SHA1 encryption algorithm with 96-bit key.

SSH user authentication is performed with passwords stored on the device or on an external authentication, authorization, and accounting (AAA) server.

The following features are not supported with SSH:

- Displaying SSH sessions
- Deleting stale SSH keys

## Telnet and SSH considerations and limitations

- Access to the switch is not allowed for both inbound Telnet and SSH connections from both IPv4 and IPv6 addresses when the Telnet or SSH server are disabled.
- Outgoing Telnet or SSH connections from the switch to any remote device is not affected by disabling or enabling the Telnet or SSH server in the switch.
- No RASLog or auditlog messages are reported when the Telnet or SSH server is disabled or enabled.

## Using DHCP Automatic Deployment

DHCP Automatic Deployment (DAD) is a method used to bring up the switch with new firmware or a preset configuration automatically.

In Network OS 4.1.0 and later, you can automatically bring up a switch with new firmware, with a preset or default configuration, omitting the need for logging in to the switch console to configure the switch. You must be using DHCP to use DAD. The DHCP process helps retrieve certain parameters (for example, the firmware path, VCS ID, VCS mode, RBridge ID, and preset configuration file) needed by the DAD process to perform the firmware and configuration downloads. If the switch is in fabric cluster mode, you can apply either the default configuration or a preset configuration. For node replacement in the logical chassis cluster mode, the switch is set to the default configuration.

You must enable DAD from the CLI, after which the switch is rebooted automatically. After the DAD process is triggered and completed, DAD is automatically disabled. If you attempt to download new firmware that is already installed on the switch, the DAD process skips the firmware download step and continues configuring the switch.

### NOTE

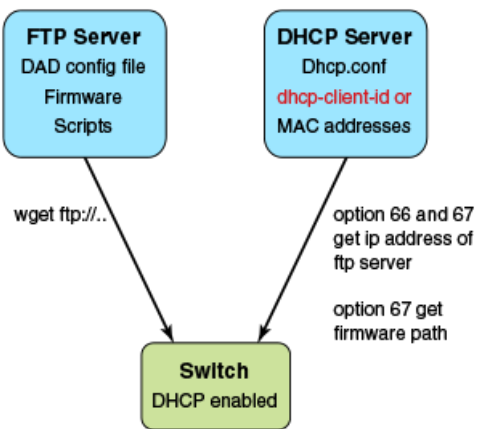
If DAD is enabled, you are warned when initiating a firmware download from the CLI that the firmware download will be unsuccessful. After a firmware download begins, DAD reports the firmware download success or failure status.

Beginning with Network OS 6.0.1, you can bring up a cluster of switches using a Python script (dad.py) for DAD. Zero Touch Provisioning (ZTP) deployment is also supported beginning with this release. When the switch is in a factory default configuration and the DHCP server for auto deployment is reachable, auto deployment is enabled automatically when the switch powers up. You can also enable DAD from the CLI, after which the switch is rebooted automatically.

#### NOTE

For more information on using Python with Network OS, refer to the "Python Event-Management and Scripting" chapter of the *Network OS Administrators guide*.

FIGURE 11 DHCP and FTP server environment for DAD



## Supported DAD use cases

DAD supports the following typical use cases:

- Invoking a firmware upgrade (and optional configuration download) on many switches at the same time in fabric cluster mode.
- Replacing a switch in a cluster by upgrading the firmware and setting up the switch to a preset configuration. In this instance, DAD must be completed on the new switch hardware (to update the firmware) before the new switch can be incorporated into the cluster.
- Logical chassis mode support for default or preset configuration. Logical chassis mode node replacement is integrated into the logical chassis mode support.
- Configuring the whole cluster using a Python script for fabric cluster mode and logical chassis mode.
- Zero Touch Provisioning (ZTP) support for IP fabrics with a single DAD configuration file for all nodes. Each of the nodes should be in the logical chassis mode with VCS ID=1 and RBridge ID=1

## Example DHCP and DAD configuration files

The following sample configuration files provide a reference for DHCP and DAD deployment environments.

The switches of a cluster are grouped together and each cluster should have its own group of switches. Each switch is added into dhcp.conf file with control parameters, such as the FTP server IP address and path to the DAD configuration file of the switch. Chassis systems support only dhcp-client-identifier, not MAC address. The following is an example file.

#### NOTE

Starting with Network OS release 7.0.0, the DHCP client identifier format in the DHCP server configuration file has changed.

In order to support firmware upgrade or downgrade between Network OS 6.0.x to 7.0.0 and later, you must update the /etc/dhcd.conf file as follows.

```
group {
  option bootfile-name "/config/unified-cfg"; # DAD config file contains settings for all switches
  option tftp-server-name "192.168.0.2";

  host cp0_new {
    option dhcp-client-identifier = "BROCADE##VDX6740##CPL2517K0FZ"; # serial number
    hardware ethernet 50:EB:1A:12:61:F3; # mac address for cp0
    fixed-address 192.168.0.88; # fixed ip address
  }
  host cp1_new {
    option dhcp-client-identifier = " BROCADE##VDX6740##CPL2517K0FZ "; # serial number
    hardware ethernet 50:EB:1A:12:61:F4; # mac address for cp1
    fixed-address 192.168.0.88; # fixed ip address
  }

  host device_chassis_new {
    option dhcp-client-identifier = " BROCADE##VDX6740##CPL2517K0FZ "; # serial number
    fixed-address 192.168.0.87; # fixed ip address
  }
}
```

### DHCP server configuration file example

The following is an example of the dhcp.conf file.

```
#ddns-update-style standard;
ddns-update-style interim;
ddns-ttl 600;
ignore client-updates; # Overwrite client configured FQHNs
ddns-domainname "infralab.com.";
ddns-rev-domainname "in-addr.arpa.";

option ntp-servers 192.168.0.2;
option domain-name-servers 192.168.0.2;
option domain-name "infralab.com";
option domain-search "infralab.com";

default-lease-time 600;
max-lease-time 7200;

authoritative;

log-facility local7;

key "rncd-key" {
  algorithm hmac-md5;
  secret "dtBgNTAoqZmwV5c4SueybjOvhe60IqgacluQrzGBv504X4nIEBEEGWrf0lCnbFhuIJXGExNBjDdNSqgBMeNI8w=";
};

subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.100 192.168.0.200;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.0.255;
  zone 0.168.192.in-addr.arpa. {
    primary 192.168.0.2;
    key "rncd-key";
  }
  zone infralab.com. {
    primary 192.168.0.2;
    key "rncd-key";
  }
}
# cluster switches
group{
```

```

option bootfile-name "/config/unified-cfg.min";
option tftp-server-name "192.168.0.2";
option routers 192.168.0.2;
# device 82
host host10 {
    option dhcp-client-identifier = "BROCADE##VDX6740##CGS0333H00R";
    hardware ethernet 00:05:33:E5:85:37;
    fixed-address 192.168.0.82;          # fixed ip address
}
host host11 {
    option dhcp-client-identifier = "BROCADE##VDX6740##CGS0333H00R";
    hardware ethernet 00:05:33:E5:85:38;
    fixed-address 192.168.0.82;          # fixed ip address
}

# device 90
host host12 {
    option dhcp-client-identifier = "BROCADE##VDX6740##CPL2549J0EG";
    hardware ethernet 00:27:F8:D2:CE:5F;
    fixed-address 192.168.0.90;          # fixed ip address
}
host host13 {
    option dhcp-client-identifier = "BROCADE##VDX6740##CPL2549J0EG";
    hardware ethernet 00:27:F8:D2:CE:5E;
    fixed-address 192.168.0.90;          # fixed ip address
}
}

```

### DAD configuration file example

The following is an example of a DAD configuration file.

```

version=3
date=10/22/2014
supported_nos=7.0.1

common_begin
vcsmode=LC
vcsid=2
rbridgeid=1
fwdir=/firmware/nos7.0.1
scriptcfgflag=2
principlerbridgeid=1
startup=/config/rbridge.cfg (shared by all switches for dhcp enable setting)
script=/script/dad.py
# 50 minute
vcstimeout=50
# 3 days = 4320 min
dadtimeout=4320
common_end

#host(device 82)
host_mac=00:05:33:E5:85:37
host_mac=00:05:33:E5:85:38
host_sn=CGS0333H00R
rbridgeid=82
defaultconfig=no
startup=/config/mc/rbridge-82.cfg
globalcfg=/config/mc/global.cfg
host_end

#host(mm 145)
host_mac=00:27:F8:46:E7:D9
host_mac=00:27:F8:38:6C:2C
host_sn=CDU2539H00L

fwdir=/min/bld/bld_dadm
rbridgeid=145
defaultconfig=no

```



```

startup=/config/mc/rbridge-145.cfg
globalcfg=/config/mc/global.cfg
host_end

#host(device 90)
host_mac=00:27:F8:D2:CE:5E
host_mac=00:27:F8:D2:CE:5F
host_sn=CPL2549J0EG

rbridgeid=90
startup=/config/mc/rbridge-90.cfg
globalcfg=/config/mc/global.cfg
defaultconfig=no
host_end

#host(device 91)
host_mac=00:27:F8:DC:1E:6B
host_mac=00:27:F8:DC:1E:6D
host_sn=CPL2501R01G

rbridgeid=91
startup=/config/mc/rbridge-91.cfg
globalcfg=/config/mc/global.cfg
defaultconfig=no
host_end

```

TABLE 10 DAD configuration file definitions

Variable	Description
<b>version</b>	<p>version 1 support from NOS4.0.0 to NOS6.0.0</p> <p>version 2 support from NOS5.0.0 to NOS6.0.0</p> <p>version 3 support NOS6.0.1+</p>
<b>date</b>	The last modification date.
<b>supported_nos</b>	The firmware version.
<b>host_mac, host_sn, host_end</b>	<p>The MAC addresses or serial number of the switch. "host_mac" or "host_sn" mark the beginning of the configuration section for a switch. The section ends with "host_end".</p> <p><b>NOTE</b> You must confirm the serial number on the switch with Brocade before adding the MAC address or serial number.</p>
<b>vcsmod</b>	VCS mode: cluster VCS mode, LC or FC.
<b>vcsid</b>	The cluster VCS ID. The range is 1 to 8192.
<b>rbridgeid</b>	<p>The unique ID for each node. When commented out with # sign, for example, "#rbridgeid=5", DAD is disabled for the node.</p> <p>If the variable <i>startup</i> is set, the value should match the configuration file set at "startup". If not, the DAD sanity check will fail. The range is from 1 to 239. You should change the default settings of vcsid=1 and rbridgeid=1.</p>
<b>principalbridgeid</b>	Principal node rbridge id of the cluster. The designated node will become the principal node of the cluster. Depending on the topology of the cluster, ideally the principal node should have direct connection to most of secondary nodes. This is ignored in ZTP mode.
<b>defaultconfig</b>	<p>Using the <b>defaultconfig</b> setting resets all the user configured settings to the factory defaults.</p> <p>If set to <i>yes</i>, the script, globalconfig, and number of nodes will be ignored and the DAD process is for single node only, not for the cluster.</p>
<b>startup</b>	<p>The local configuration file. The value can be <i>default</i> or <i>configuration file</i>. If the variable <i>defaultconfig</i> is set to <i>yes</i>, <i>startup</i> should be commented out or set empty. If not the DAD sanity check will fail.</p> <ul style="list-style-type: none"> <li>For NOS 6.0.0 and prior releases this means the switch running configuration. It must be uploaded from each switch with NOSCLI copy running-config ftp://... command.</li> </ul>

TABLE 10 DAD configuration file definitions (continued)

Variable	Description
	<ul style="list-style-type: none"> <li>For NOS 6.0.1 and later releases, this means the local configuration only.</li> </ul>
<b>globalcfg</b>	The cluster global configuration file. This is only set for the DAD principal node and will be ignored by secondary nodes. This should be either set empty or a valid configuration file path must be specified. This is created using the <code>copy global-running-config ftp://...</code> command.
<b>scriptcfgflag</b>	<p><b>defaultconfig</b> must be set to <i>no</i>. This is not a mandatory variable. The default is 0, when not specified. The meaning of the value is:</p> <p>0 - only use startup and globalcfg, script is ignored</p> <p>1 - only use script, startup and globalcfg are ignored</p>
<b>script</b>	The set up script file.
<b>ztp</b>	ZTP mode: 1 - enabled (default), 0 - disabled. When enabled, it changes the behavior of DAD. Only the settings in the "common" section are used. The "host" section are ignored. <code>vcsmode=LC</code> will be forced. These settings in the configuration file will be ignored.
<b>fwdir</b>	Firmware path in FTP server. If set to empty, DAD will skip firmware download.
<b>common_begin, common_end</b>	The setting in the section will be shared by all switches.

## Configuring the DAD process for replacing data center fabric switches

Use the following procedure to configure DHCP Automatic Deployment (DAD) when replacing data center fabric switches that are in logical chassis cluster mode.

For data center fabric switches that are in logical chassis cluster mode, the DAD process applies to a new switch and the principal switch. (An IP Fabric supports logical chassis cluster mode only.)

1. Disconnect the existing switch from the cluster.
2. Connect the new switch to the cluster. The new switch must be the same model and use the same cable connection as the old switch.  
The new switch must successfully load Network OS. Note, however, that the new switch cannot join the cluster just yet.
3. From the principal switch, manually run the node replacement with the WWN and RBridge ID.
4. Establish a DAD environment for the new switch. (Make sure DHCP is enabled on the management interface.)
  - The management interface of the switch must be set up as DHCP. After setting up the management interface on a switch in fabric cluster mode, you must use the **copy running-config startup-config** command for the configuration to take effect.
  - The DHCP server must have the FTP server IP address and configuration file path.
  - The configuration file is on the FTP server and it contains the firmware path, new configuration file path, VCS ID, VCS mode, and RBridge ID.
  - The DHCP server and FTP server must be up and running.
  - DAD must be enabled on the switch by means of the CLI.
5. Enable DAD by using the **dhcp auto-deployment enable** command, and enter **yes** when prompted to reboot the system. After the new switch is rebooted, the DAD process downloads the DAD configuration file to get the VCS mode, VCS ID, and RBridge ID. The RBridge ID must be configured the same as the previous node in the cluster. The DAD process sets the VCS ID and RBridge ID for a switch in logical chassis cluster mode. No reboot is triggered. The DAD process invokes a firmware download if new firmware is detected. Firmware download completes successfully and the switch comes up with the new firmware and configuration settings. Note that the DAD process aborts if any error is detected. When the new switch comes up, it joins the cluster with the same configuration as the previous switch.
6. Use the **show dadstatus** command to view the current DAD configuration.

### Considerations for enabling DHCP auto-deployment

The **dhcp auto-deployment enable** command causes a cold/disruptive reboot and requires that Telnet, secure Telnet, or SSH sessions be restarted.

1. Scenario 1: When you enable DAD and the system starts to reboot, the DAD process is triggered after configuration replay is complete.  
For dual management module (MM) chassis (VDX 8770 chassis), the DAD process waits for the dual MM to be in sync before starting the requested firmware download. However, if you manually issue **firmwaredownload -sb** during this period (after DAD is triggered and before MM is in sync), DAD fails because the previous firmware download takes precedence. If you manually issue **firmwaredownload -sb** before DAD is triggered, DAD will fail for the same reason.
2. Scenario 2: You issue the command to enable DAD (answer "Yes" when prompted), but before the system reboot, there is an HA failover. DAD will be cancelled. You must enable DAD from the new active switch.
3. Scenario 3: You issue the command to enable DAD, but after the system reboot is invoked, takeover occurs (the previous standby switch becomes the new active switch), DAD will proceed.
4. Scenario 4: You manually issue the **firmwaredownload** command, but before the firmware download is completed, you enable DAD from the CLI and answer "Yes" when prompted to reboot the switch. When the switch boots up, even if the DAD process detects that the firmware download is needed, it will fail during the sanity check because the previous incomplete firmware download takes precedence. DAD fails.
5. Scenario 5: If you do not power down the secondary node when running DAD on the principal node, the following outcomes are observed:
  - The DAD principal node and secondary node form the cluster, but without the principal role. DAD fails on the principal node.
  - The DAD principal node and secondary node form the cluster with the principal role. DAD proceeds on the principal node because the secondary node does not affect DAD.
  - The DAD principal node and secondary node do not form the cluster. DAD proceeds on the principal node because the secondary node does not affect DAD.

### Configuring the DAD process for fabric cluster switches (for VCS Fabrics only)

For fabric cluster switches, the DHCP Automatic Deployment (DAD) process is applicable to both cluster upgrades and node replacement.

The following procedure configures DAD on switches in fabric cluster mode.

1. Establish a DAD environment for the new switch. (Make sure DHCP is enabled on the management interface.)
  - The management interface of the switch must be set up as DHCP. After setting up the management interface on a switch in fabric cluster mode, you must use the **copy running-config startup-config** command for the configuration to take effect.
  - The DHCP server must have the FTP server IP address and configuration file path.
  - The configuration file is on the FTP server and it contains the firmware path, new configuration file path, VCS ID, VCS mode, and RBridge ID.
  - The DHCP server and FTP server must be up and running.
  - DAD must be enabled on the switch by means of the CLI.
2. Enable DAD by using the **dhcp auto-deployment enable** command, and enter **yes** when prompted to reboot the system. During system bootup, the DAD process downloads the DAD configuration file and obtains the VCS ID and RBridge ID settings for a switch in fabric cluster mode. The switch configuration is retrieved from the FTP server if the FTP server is set up.

**NOTE**

The DAD process aborts if any error is detected.

3. If the node configuration must be downloaded, set up the new configuration as the startup configuration so it will be applied automatically.  
The DAD process invokes a firmware download if new firmware is detected. Once the firmware download completes successfully, the switch comes up with the new firmware and configuration settings.
4. Use the **show dadstatus** command to view the current DAD configuration.

**DAD configuration considerations**

Note the following general considerations when using DAD:

- The DAD process is disruptive to traffic.
- Currently, only DHCPv4 is supported.
- Configuration download is not supported during a firmware downgrade.
- Configurations are not downloaded if the DAD process is aborted due to a sanity check failure, or if you are downloading the same firmware version.
- If an existing firmware download session is either occurring or paused, such as during a firmware commit, DAD is not triggered. Instead, the last firmware download session continues. If a firmware download is in progress and you attempt to enable DAD, you are prompted to try again later.
- In-Service Software Upgrade (ISSU) is not supported at this time.
- For dual management module (MM) chassis (VDX 8770 chassis), the dual MM must be in sync from the chassis bootup (not from HA failover). In a chassis system, both MMs are rebooted at the same time.
- DAD is not supported in FIPS mode.
- You can choose to apply either the default configuration or the preset configuration.
- DAD must be enabled on the principal node first. All the other nodes must be enabled in parallel.
- The preset configuration can be either a configuration file or a running setup script.
- Cluster principal node failover is not supported.
- Adding a node into an existing cluster is not supported.
- DAD over in-band is not supported.
- Virtual Fabrics is not supported with DAD. You must disable Virtual Fabrics before starting the DAD process in the global configuration file or in the script.
- If switches are already configured with virtual fabric, this configuration will not be changed by the DAD process. Similarly, other global configurations that are not modified by the **copy default to startup** command will not be modified by DAD either.

**DAD using the Python script**

The Python script `dad.py` allows you to configure the switch cluster with preset configuration files.

This Python script configuration method reduces the time taken for firmware download, switch configuration, and cluster formation for the fabric cluster mode and logical chassis mode. Because all switches download the same firmware and the cluster parameters remain consistent across all switches, using the Python script is a more scalable method for deployment and reduces potential human error.

Once you enable DAD on the switch, the DAD process calls the `dad.py` script from the FTP server. The `dad.py` script starts running whenever the number of nodes detected in the fabric equals the number of nodes that have joined the cluster. The DAD process monitors the nodes.

### Python script support considerations for DAD

- The **reboot** command is not supported in the Python script.
- If the switch has a preset local configuration, the script will overwrite it.
- The start and completion times of the script will be reported, although script internal errors will not be reported. You must check the internal errors manually.
- If you change the DAD configuration script on any node in the cluster, the switch cluster must run the DAD process again.
- To make the configuration change persistent, if there is a change in the fabric cluster mode, use the **copy running-config startup-config** command.
- The cluster DAD process has a time limit (three days) to run the script. If the number of nodes in the cluster is not equal to what is specified in the DAD configuration file, the principal node declares DAD partially complete after timeout. If the deployment fails on the secondary node, you must restart the deployment again before the principal node deployment times out.
- The global configuration replay takes place in parallel with firmware download. The global configuration file may take a long time to execute if it is big. However, the DAD status will display as complete when firmware download completes. You must manually check if the configuration file is executed completely. If the configuration file is not fully executed, the DAD status still remains complete and not failed.
- If the secondary node triggers a firmware download, the principal node will trigger the Python script once the secondary node joins the cluster. The firmware download on the secondary node continues in parallel and may complete after the principal node declares DAD complete.

### DAD on the principal node

The following steps describe the procedure for DAD enabled by the dad.py Python script for the logical chassis and fabric cluster mode. The dad.py Python script runs once you enable DAD on the switch.

#### NOTE

Refer to the "Script for upgrading and reconfiguring switches" section in the *Network OS Administration Guide* for more information on the dad.py script.

The following prerequisites apply to the DAD process.

- Set up the FTP server directory structure containing the firmware, Python script or the switch configuration file.
- Create the DAD configuration file for the cluster, such as the VCS mode, VCS ID, RBridge ID etc. Then upload the file to the FTP server.
- In the DAD configuration file, for the RBridge ID, you should change the values from the default settings of VCS ID=1 and RBridge ID=1. The globalcfg should be set only for the DAD principal node, and left empty for the secondary nodes.
- Set up the DHCP server configuration to assign fixed IP addresses to each switch and DAD configuration file for each switch.

The principal node in the logical chassis cluster completes the DAD as a standalone node first.

1. Power down all the secondary nodes in the cluster.
2. Enable DHCP. If the switch is currently in the fabric cluster mode, use the **copy running-config startup-config** command.
3. Enable DAD using the **dhcp auto-deployment enable** command.

Once you enable DAD on the switch, the following process begins. For the logical chassis mode, the run order of the script is 3, 1, 2 on the principal node.

1. global - Run logical chassis cluster global configuration commands from the principal node.
2. rbridge-id 2 - Configuration commands for a specific node run from the principal node.
3. rbridge-id 2 - local - Configuration commands allowed to be run from the local node.

Check on the deployment progress until the process is complete. If any of the switches fail the process, you will need to run the process again before the principal node deployment times out.

### DAD on the secondary node

Once the principal node deployment completes successfully, the DAD process starts on the secondary node.

1. Enable DHCP. If the switch is in fabric cluster mode, use the **copy running-config startup-config** command. Make sure the local time of the switch is in sync with the principal node.
2. Enable DAD using the **dhcp auto-deployment enable** command.

Once you enable DAD on the switch the DAD process begins. For the fabric cluster mode, the script runs on the local configuration (--rbridgeid #). For the logical chassis mode, the script runs on the local configuration (--rbridgeid # --local).

#### NOTE

Use the **show dadstatus** command to view the status of the DAD process as it runs.

## DHCP zero touch provisioning

Zero touch provisioning (ZTP) allows you to automatically start up the device with the correct firmware and configuration as soon as you plug into the network.

The following configuration considerations apply to DAD in a ZTP environment.

- Single DAD configuration file per IP fabric.
- ZTP is supported only on out-of-band ports.
- In an IP fabric, all nodes will have the same VCS ID and RBridge ID in the logical chassis mode.
- A VCS cluster is not formed among any nodes.
- You must set the IP address for each switch in the DCMD configuration file with "startup" setting in the DAD configuration file or with the script.
- All nodes can either be powered up at the same time or enabled from the CLI.
- DAD executes only if the switch configuration is the default configuration. If the configuration on the switch is not the default configuration, DAD exits.
- If the switch is in the default configuration before DAD is triggered, DHCP will remain enabled after the deployment completes. However, this setting can be overwritten by the switch-specific configuration file or the dad.py script.
- The factory default DAD runs only once in a DHCP-enabled environment. Irrespective of whether this process is a success or failure, DAD will not be triggered again after a reboot or power off. You can run DAD manually using the **dhcp auto-deployment enable** command if required.
- DAD is enabled automatically upon switch reboot when you use the **write erase** command.

### Using zero touch provisioning

The following steps describe the DHCP zero touch provisioning deployment process.

You must first adhere to these pre-requisites for the zero touch provisioning deployment process.

- Do not use vcsid=1. This is preserved for the factory default.
- DHCP is enabled from the startup configuration by setting the "startup" value.
- The host specific section will be ignored.
- Set the value "ztp=1" in the DAD configuration file.

- Set the value `scriptcfgflag=2` when the script is configured; set the value `scriptcfgflag=0` when script is not configured.
  - In scenarios where zero touch provisioning is not used, you must mandatorily set "`ztp=0`", because ZTP is enabled by default if you do not specify this value.
  - When using the script, the script should contain the IP address (static IP address with DHCP gateway) set up on the management interface.
1. Power up the switch, or run the **write erase** command from the CLI prompt.
  2. When the switch boots up, check if the DHCP server is available. If the DHCP server is unavailable, the ZTP process aborts without reporting an error.
  3. Disable the bare metal mode on the switch.
  4. Enable DHCP once the switch reboots.  
Once you enable DHCP, the zero touch provisioning process starts. The `dad.py` script runs on the global and local configuration for zero touch provisioning on the node.

## Ethernet management interfaces

The Ethernet network interface provides management access, including direct access to the Network OS CLI. You must configure at least one IP address using a serial connection to the CLI before you can manage the system with other management interfaces. You can either configure static IP addresses, or you can use a Dynamic Host Configuration Protocol (DHCP) client to acquire IP addresses automatically. For IPv6 addresses, both static IPv6 and stateless IPv6 autoconfiguration are supported.

### ATTENTION

Setting static IPv4 addresses and using DHCP are mutually exclusive. If DHCP is enabled, remove the DHCP client before you configure a static IPv4 address. However, this does not apply to IPv6 addresses.

## Brocade VDX Ethernet interfaces

The Brocade VDX Top-of-Rack (ToR) switches have a single configurable Ethernet interface, `Eth0`, which can be configured as a management interface.

The modular chassis, the Brocade VDX 8770-8 and the Brocade VDX 8770-4, have two redundant management modules, MM1 and MM2. Each management module can communicate with each of the line cards (interface modules) through an Ethernet connection. Each management module has two Ethernet interfaces, `Eth0` and `Eth2`. These interfaces are also known as out-of-band (OOB) management interfaces.

`Eth0` is the management interface and can be configured with an IP address. `Eth2` provides connectivity to the other management module and the line cards in the chassis. The `Eth2` IP addressing scheme uses default IP addresses to communicate between the modules; these addresses are not user-configurable.

To set a virtual IP or IPv6 address for the chassis, use the **chassis virtual-ip** or **chassis virtual-ipv6** command in RBridge ID configuration mode.

### NOTE

The IP address of the management platform must be in the same subnet as the devices it manages. It can be configured only in the same subnet that supports the out-of-band management module interfaces, and it cannot be used in the same subnet that supports a virtual Ethernet (VE) interface.

## Lights-out management

Lights-out management (LOM) is the ability for a system administrator to monitor and manage servers by a LOM remote control program.

A complete LOM system consists of a hardware component called the LOM module and a program that facilitates the continuous monitoring of variables such as microprocessor temperature and utilization. The program also allows for such remote operations as rebooting, shutdown, troubleshooting, alarm setting, fan-speed control, and operating system reinstallation.

The modular chassis, the Brocade VDX 8770-8 and the Brocade VDX 8770-4, have two redundant management modules, MM1 and MM2. Each management module can communicate with each of the line cards (interface modules) through an Ethernet connection. Each management module has two Ethernet interfaces, Eth0 and Eth2. These interfaces are also known as Out of Band (OoB) management interfaces and support LOM programs.

## Stateless IPv6 autoconfiguration

IPv6 allows the assignment of multiple IP addresses to each network interface. Each interface is configured with a link local address in almost all cases, but this address is only accessible from other hosts on the same network. To provide for wider accessibility, interfaces are typically configured with at least one additional global scope IPv6 address. IPv6 autoconfiguration allows more IPv6 addresses, the number of which is dependent on the number of routers serving the local network and the number of prefixes they advertise.

When IPv6 autoconfiguration is enabled, the platform will engage in stateless IPv6 autoconfiguration. When IPv6 autoconfiguration is disabled, the platform will relinquish usage of any autoconfigured IPv6 addresses that it may have acquired while IPv6 autoconfiguration was enabled. This same enabled and disabled state also enables or disables the usage of a link local address for each managed entity (though a link local address will continue to be generated for each switch) because those link local addresses are required for router discovery.

The enabled or disabled state of autoconfiguration does not affect any static IPv6 addresses that may have been configured. Stateless IPv6 autoconfiguration and static IPv6 addresses can coexist.

## Switch attributes

A switch can be identified by its IP address, World Wide Name (WWN), switch ID or RBridge ID, or by its host name and chassis name. You can customize the host name and chassis name with the **switch-attributes** command.

- A host name can be from 1 through 30 characters long. It must begin with a letter, and can contain letters, numbers, and underscore characters. The default host name is "swO." The host name is displayed at the system prompt.
- Brocade recommends that you customize the chassis name for each platform. Some system logs identify the switch by its chassis name; if you assign a meaningful chassis name, logs are more useful. A chassis name can be from 1 through 30 characters long, must begin with a letter, and can contain letters, numbers, and underscore characters. The default chassis names are based on the switch models, such as is VDX 8770-4 or VDX 8770-8.

## Switch types

The *switchType* attribute is a unique device model identifier that is displayed when you issue the **show chassis** or the **show rbridge-id** commands. When you are gathering information for your switch support provider, you may be asked for the Brocade product name. Use the information in the following table to convert the switchType identifier to a Brocade product name.



**TABLE 11** Mapping switchType to Brocade product names

switchType	Brocade product name	Description
112	Management Module	Internal component on the switch
113	Switch Fabric Module	Internal component on the switch
155	VDX 2741	10Gb scalable switch for the BR-VDX2741 chassis, based on the VDX 6740 ToR switch. 42 x 10GbE internal, 14 x 10GbE/16G FC + 2 x 40GbE/64G FC external FlexPorts
138	VDX 2746	10Gb scalable switch for the Hitachi BS2500 chassis, based on the VDX 6740 ToR switch. 42x10GbE internal, 14x10GbE/16G FC + 2x40GbE/64G FC external FlexPorts.
131	VDX 6740	48 10-GbE SFP+ ports and 4 40-GbE QSFP+ ports
137	VDX 6740T	48 10-GbE 10BASE-T ports and 4 40-GbE QSFP+ ports
138	VDX 6746	10Gb scalable switch for Hitachi CB2500 chassis based on the VDX 6740 ToR switch. 42 x 10GbE internal, 14 x 10GbE/16G FC + 2 x 40GbE/64G FC external FlexPorts
151	VDX 6740T-1G	Same as VDX 6740T, but ships with ports set to 1 GbE
153	VDX 6940-36Q	36 40GbE QSFP+ ports
1000.x	VDX 8770-4	4 I/O slot chassis supporting 48x1 GbE, 48x10 GbE, 48x10G-T, 12x40 GbE, 27x40 GbE, or 6x100 GbE line cards
1001.x	VDX 8770-8	8 I/O slot chassis supporting 48x1 GbE, 48x10 GbE, 48x10G-T, 12x40 GbE, 27x40 GbE, or 6x100 GbE line cards

## Operational modes

Network OS supports the following operational modes for Brocade VDX switches.

The two operational modes are:

- *Logical chassis cluster mode* — This mode requires Network OS 4.0.0 or later. In this mode, both the data and configuration paths are distributed through the VCS Fabric. The entire cluster is configured from the principal node. Refer to [Logical chassis cluster mode](#) on page 58 for more information.
- *Fabric cluster mode* — In this mode, the data path for nodes is distributed, but the configuration path is not distributed. Each node keeps its configuration database independently. Refer to [Fabric cluster mode \(VCS Fabrics only\)](#) on page 60 for more information. Fabric cluster mode is not supported in an IP Fabric.

When a new switch boots up, the switch enters logical chassis cluster mode.

### ATTENTION

The generic term *VCS mode* in this manual applies to both fabric cluster mode and logical chassis cluster mode unless otherwise stated.

Each time you change the Brocade VCS Fabric configuration, the switch resets to the default configuration and reboots automatically. Make sure to save the configuration before you change it.

## Logical chassis cluster mode

Logical chassis cluster mode is defined as a fabric in which both the data and configuration paths are distributed. The entire cluster must be globally configured from the principal node. Logical chassis cluster mode requires Network OS 4.0.0 or later.

### Logical chassis cluster mode support for platforms

The following platforms support logical chassis cluster mode and is used in any combination:

- Brocade VDX 2741
- Brocade VDX 2746
- Brocade VDX 6740
- Brocade VDX 6740T
- Brocade VDX 6740T-1G
- Brocade VDX 6940-36Q
- Brocade VDX 6940-144S
- Brocade VDX 8770-4
- Brocade VDX 8770-8

### Logical chassis cluster mode characteristics

The following are the main characteristics of logical chassis cluster mode:

- The maximum number of nodes supported in a logical chassis cluster is 48.
- This mode supports in-band management (through ethO on management modules) over virtual Ethernet (VE) interfaces.
- In-Band Management is supported in Logical Chassis mode on VDX devices.
- If you use in-band management only, and wish to disable the management interface (which is considered *out of band*), refer to the **shutdown** (interface) command in the *NOS Command Reference*.
- Physical connectivity requirements for logical chassis cluster deployment are the same as those for fabric cluster deployment.
- A single global configuration exists across all nodes, while each node can contain its unique local configuration. However, each node contains the local configuration information for all other nodes in the cluster.
- When an RBridge is rejoining the logical chassis cluster, the interface-level configuration is reset to the default values.
- Global and local configurations for the entire logical chassis cluster are performed from one node —the principal node only.
- Startup configurations are not maintained by the cluster; each node preserves its running configuration.
- A logical chassis cluster can be transitioned into a fabric cluster while preserving configurations, if you follow the steps provided later in this section
- An existing fabric cluster can be transitioned into a logical chassis cluster while preserving configurations, if you follow the steps provided later in this section
- Cluster-wide firmware upgrades can be performed.
- Cluster-wide supportSave can be performed.

### Command blocking in logical chassis cluster mode

In logical chassis cluster mode, some commands cannot be run while other commands or events are processing.

If one of the following CLI command types or events is in progress in the cluster, then any one of the CLI command types in the following list will be rejected until the current command or event has finished.

1. **Copy file running-config** commands
2. HA failover commands
3. VCS ID/RbridgeID change commands
4. Cluster mode change from logical chassis cluster to fabric cluster
5. **Copy default-config startup-config** commands
6. Configuration updates by individual commands
7. Cluster formation events, such as initial cluster formation or secondary joining or rejoining of a cluster

These commands and events are considered to be blocked from occurring simultaneously. However, if the principal node changes during one of these operations or HA failover occurs on principal switch, the new principal will not retain the information that the commands or events not in progress are in a blocked state.

In the case of commands being blocked, the following messages are some of the error messages that could result:

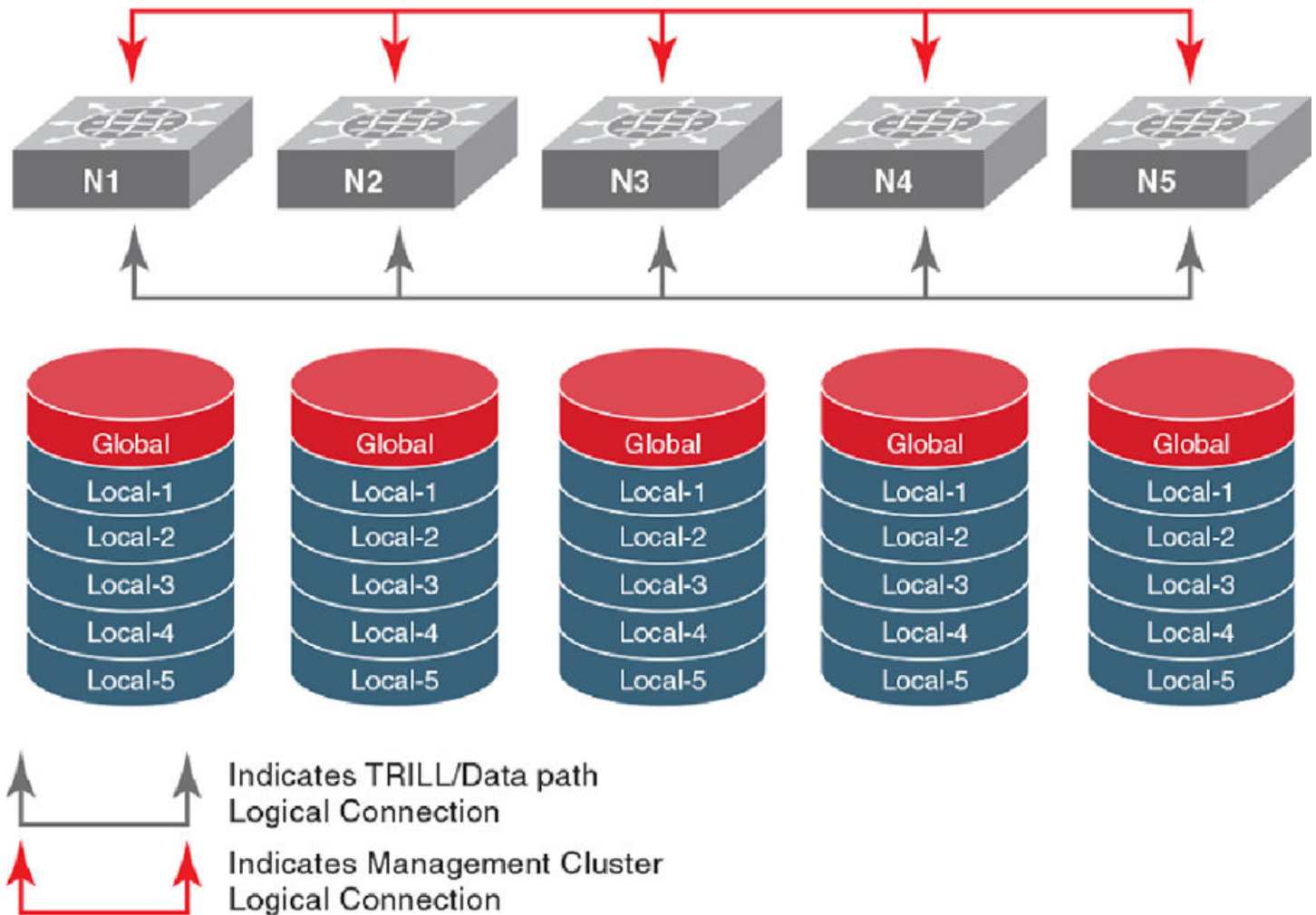
- Cluster formation is in progress. Please try again later.
- User Configuration update is in progress. Please try again later.
- Configuration file replay is in progress. Please try again later.
- HA failover is in progress in the cluster. Please try again later.
- VCS Config change is in progress in the cluster. Please try again later.
- Copy default-config startup-config is in progress. Please try again later.

## Logical chassis cluster mode configuration

In logical chassis cluster mode, any operation that results in writing to the configuration database gets automatically distributed. There are no exceptions.

Each node in the logical chassis cluster maintains an individual copy of the configuration to enable high availability of the cluster. The following figure illustrates nodes in a logical chassis cluster. Each node has its own databases, and the databases kept by each node are identical at all times.

FIGURE 12 Configuration database in a logical chassis cluster



Network OS switches contain both global and local configuration. In a logical chassis cluster, a single global configuration exists across all cluster members, while each individual member has its own local configuration. (Conversely, in fabric cluster mode, each cluster member can have its own unique global configuration.)

Global configuration is required for cluster-wide operations, whereas local configuration is specific to the operation of an individual node. For more information and examples of each type of configuration, refer to [Examples of global and local configurations](#) on page 83.

### Fabric cluster mode (VCS Fabrics only)

Fabric cluster mode is defined as a fabric in which the data path for nodes is distributed, but the configuration path is not distributed. Each node keeps its configuration database independently.

By default, the switch will boot up in fabric cluster mode and will attempt to form Inter-Switch Links (ISLs):

If the chassis is not connected to another switch, it forms a "single node VCS fabric." This means that the chassis operates as a standalone system, but the operational mode is always VCS-enabled. You cannot disable the VCS mode on any of the models listed above.

#### NOTE

In fabric cluster mode, the **all** keyword to the **rbridge-id** command is not available, and a remote RBridge cannot be addressed by means of the **rbridge-id rbridge-id** command.

## Transitioning between modes (VCS Fabrics only)

The **vcs set-rbridge-id** command allows you to change the RBridge ID or optionally the VCS ID of a node, and also to transition the node from logical chassis cluster mode to fabric cluster mode, or back to logical chassis cluster mode again.

#### ATTENTION

Each time you change the Brocade VCS Fabric configuration, the switch resets to the default configuration and reboots automatically. Make sure to save the configuration before you issue this command.

To change the RBridge ID of a node to 10:

```
device# vcs set-rbridge-id 10
```

To change the RBridge ID of a node to 10 and its VCS ID to 35:

```
device# vcs set-rbridge-id 10 vcsid 35
```

To convert a node that is in fabric cluster mode to logical chassis cluster mode, while simultaneously changing its RBridge ID to 10 and its VCS ID to 35:

```
device# vcs set-rbridge-id 10 vcsid 35 logical-chassis enable
```

To convert a node that is in logical chassis cluster mode to fabric cluster mode, while optionally simultaneously changing its RBridge ID to 10 and its VCS ID to 35:

```
device# no vcs set-rbridge-id 10 vcsid 35 logical-chassis enable
```

#### NOTE

You can also use the **no vcs logical-chassis-enable** command without the option of setting the RBridge ID and VCS ID.

## Modular platform basics

The Brocade VDX 8770 platform features two redundant management modules, three or six switch fabric modules, and four or eight line cards depending on the switch model. The Brocade VDX 8770-4 supports four line cards and the Brocade VDX 8770-8 supports eight line cards.

The following table lists the modules supported on each platform.

**TABLE 12** Modules supported on the Brocade VDX 8770 platform

Type MM	Module ID	Slot numbers VDX 8770-4	Slot numbers VDX 8770-8	Description
	0x70 = 112	M1, M2	M1, M2	Management module (an 8-core 1.5-GHz Control Processor)
SFM	0x71 = 113	S1 - S3	S1 - S6	Switch fabric module (core blade)

**TABLE 12** Modules supported on the Brocade VDX 8770 platform (continued)

Type MM	Module ID	Slot numbers		Description
		VDX 8770-4	VDX 8770-8	
LC48X10G	0x72 = 114	L1 - L4	L1 - L8	48-port 10-GbE line card
LC12X40G	0x7F = 127	L1 - L4	L1 - L8	12-port 40-GbE line card
LC48X1G	0x83 = 131	L1 - L4	L1 - L8	48-port 1-GbE line card
LC48X10G-T	0x97 = 151	L1 - L4	L1 - L8	48-port 10 Gbps Base-T line card
LC27X40G	0x96 = 150	L1 - L4	L1 - L8	27-port 40-GbE line card
LC6X100G	0x95 = 149	L1 - L4	L1 - L8	6-port 100-GbE line card

## Management modules

Two management modules (MMs) provide redundancy and act as the main controller on the Brocade VDX 8770-4 and VDX 8770-8 chassis. The management modules host the distributed Network OS that provides the overall control plane management for the chassis. You can install a redundant management module in slot M1 or M2 in any of the Brocade VDX 8770 chassis. By default, the system considers the module in slot M1 the active management module and the module in slot M2 the redundant, or standby, management module. If the active module becomes unavailable, the standby module automatically takes over management of the system.

Each management module maintains its own copy of the configuration database. The startup configuration is automatically synchronized with the other management module.

Brocade recommends that each management module (primary and secondary partition) should maintain the same firmware version. For more information on maintaining firmware, refer to the “Installing and Maintaining Firmware” section of the *Network OS Upgrade Guide*.

Each management module has two Ethernet interfaces, Eth0 and Eth2. Eth0 is the management interface and can be configured with an IP address. For more information on configuring the management interface, refer to [Connecting to a switch](#) on page 43.

## HA failover

Warm-recovery High Availability (HA) failover is supported for both fabric cluster mode and logical chassis cluster mode.

Warm recovery includes the following behaviors:

- No data path disruption results for Layer 2, Layer 3 and FCoE traffic.
- All Layer 2 and Layer 3 control protocol states are retained.
- The topology state and interface state are retained.
- All running configuration is retained (including the last accepted user configuration just before HA failover).
- During a warm recovery, the principal switch in a logical chassis cluster remains the principal switch. After warm recovery, the principal switch reestablishes cluster management layer connection with other switches and reforms the cluster.
- A secondary switch in a logical chassis cluster reestablishes cluster management layer connection with the principal switch and rejoins the cluster after warm recovery.
- If you run a **reload** command on an active MM, the principal switch in a logical chassis cluster goes into cold recovery and comes back up as a secondary switch.
- HA behavior during In-service software upgrades is the same as for warm-recovery failover.

### NOTE

The **ha failover** command is supported only on a dual-management-module chassis system.

## Support for in-service software upgrades

Refer to the respective NOS-version release notes for ISSU and upgrade-path information. An ISSU allows a dual management module system or Top of Rack switches to be upgraded non-disruptively and is invoked by entering the **firmware download** command from the active management module. ISSU is not supported in NOS 6.0.0 from previous NOS versions. Use the coldboot or manual options of the **firmware download** command.

High Availability behavior during ISSUs is the same as that of warm recovery described in [HA failover](#) on page 62. For more information, refer to the “Upgrading firmware on a modular chassis” of the *Network OS Upgrade Guide*.

## Enabling/disabling standby MM console input

Use the key sequences shown in this section to either allow or prevent user console input.

By default, the standby MM console does not accept any key inputs. Using a special key sequence, you can enable /disable key-access input on the standby MM after HA synchronization is established.

Use the following keyboard sequences to disable and enable console user input:

- To enable input: ctrl \_ 1 (ctrl underscore and 1)
- To disable input: ctrl \_ O (ctrl underscore and O)

Situations in which console user input becomes enabled are:

- Whenever an MM becomes active due to cold start or warm start.
- If the HA is out of sync for any reason.

## Switch fabric modules

The switch fabric modules play a dual role in the fabric connectivity between line cards, providing both the data-plane connectivity and the control-plane connectivity needed for end-to-end credit management in each of the line cards.

In each chassis model, two slots are designated for supporting the control-plane connectivity. In the Brocade VDX 8770-4, the slots S1 and S2 are the designated control-plane slots. In the Brocade VDX 8770-8, the slots S3 and S4 are the designated control-plane slots. At least one of the control-plane slots must be populated to maintain operation. If you remove the switch fabric modules from both the control-plane slots, all line cards will be faulted and the chassis is no longer operational.

## Line cards

The following line cards provide I/O ports for network Ethernet protocols:

- LC48x1G - forty eight 1-GbE/10-GbE SFP+ front ports.
- LC48x10G - forty eight 1-GbE/10-GbE SFP+ front ports.
- LC12x40G - twelve 40-GbE QSFP front ports.
- LC48x10G-T - forty eight 10 Gbps Base-T front ports.
- LC27x40G - twenty seven 40-GbE QSFP front ports.
- LC6x100G - six 100-GbE front ports.

## Supported interface modes

All interfaces in Brocade VDX chassis come online as Fabric Inter-Switch Links (“Fabric ISLs”) by default and will attempt to form a Brocade VCS fabric. If the ISL formation fails, the interfaces come up as “Edge ports”.

## Slot numbering and configuration

The slot number specifies the physical location of a module in a switch or router, and the number of available slots of each type (interface, management, or switch fabric) depends on the router. Slot configuration is done on a slot-by-slot basis, and the configurations are stored in a persistent database on the switch.

### Slot numbering

The slot numbering on the Brocade VDX 8770 chassis is based on the module type. The slot numbers for the line card are numbered L1 through L4 on the Brocade VDX 8770-4, and L1 through L8 on the Brocade VDX 8770-8. The slots for the management modules are numbered M1 and M2. The slots for the switch fabric modules are numbered S1 through S3 on the Brocade VDX 8770-4, and S1 through S6 on the Brocade VDX 8770-8.

### Slot configuration

Line cards are registered with the system by type, and the slot must be configured with the correct type before you can install a line card in that slot. When you install a new line card, the system checks whether or not a previous configuration is associated with the slot. The following rules apply when you install or replace a line card:

- When you install a line card and boot it up to an online state in a slot that was never occupied or configured, the module type information is automatically detected and saved to the database. No special configuration is required.
- If you install a line card in a slot that was previously occupied by a line card of the same type and the slot is configured for that same type, you can hot-swap the modules without powering off the line cards. No slot configuration changes are required.
- If the slot was previously configured for a different type of line card, the installation fails and the module is faulted with a "Type mismatch" error. A RASLog error message is generated. You must power off the line card and clear the slot configuration with the **no linecard** command before you can configure the slot for a new line card.

The slot configuration persists in the database even after the line card is physically removed, powered off, or faulted since it first came online. All configuration data associated with the slot is automatically preserved across reboot or hot-swap of the line card with the same type.

## Connecting to a switch

You can connect to your switch through a console session on the serial port. Also, you can use SSH or telnet to connect to the management port. You can also use SSH and telnet to connect to an IP inband interface configured on an Ethernet port, a VE interface, or loopback in the mgmt-vrf (management VRF) or default-vrf. You can use any account login present in the local switch database or on a configured authentication, authorization, and accounting (AAA) server for authentication. For initial setup procedures, use the preconfigured administrative account that is part of the default switch configuration.

The switch must be physically connected to the network. If the switch network interface is not configured or the switch has been disconnected from the network, use a console session on the serial port.

- Refer to the Brocade VDX hardware reference manuals for information on connecting through the serial port.
- Refer to [Configuring Ethernet management interfaces](#) on page 68 for details on configuring the management interface.

## Establishing a physical connection for a Telnet or SSH session

1. Connect through a serial port to the switch.
2. Verify that the switch's network interface is configured and that it is connected to the IP network through the RJ-45 Ethernet port.



- Log off the switch's serial port.
- From a management station, open a Telnet or SSH connection using the management IP address of the switch to which you want to connect.

For more information on setting the management IP address, refer to [Connecting to a switch](#) on page 43.

- Enter the password.

Brocade recommends that you change the default account password when you log in for the first time. For more information on changing the default password, refer to the *Brocade VDX Hardware Reference* manuals.

- Verify that the login was successful.

The prompt displays the host name followed by a pound sign (#).

```
switch# login as: admin
admin@10.20.49.112's password:*****

-----
SECURITY WARNING: The default password for at least
one default account (root, admin and user) have not been changed.
Welcome to the Brocade Network Operating System Software
admin connected from 10.110.100.92 using ssh on VDX 6740-48
```

## Telnet services

You can use the Telnet service to connect to a switch using either IPv4 or IPv6 protocol.

### Establishing a Telnet connection

A Telnet session allows you to access a switch remotely using port 23. However, it is not secure. If you need a secure connection, use SSH.

- To establish a Telnet session connection, enter **telnet** followed by the switch IP address.

```
switch# telnet 10.17.37.157
```

If the switch is active and the Telnet service is enabled on it, a display similar to the following will appear.

```
Trying 10.17.37.157...
Connected to 10.17.37.157.
Escape character is '^]'.
Network OS (sw0)
switch login:
```

- Once you have established the Telnet connection, you can log in normally.

#### NOTE

You can override the default port by using the **telnet ip\_address** command with the optional **port** operand (range 0-65535). However, the device must be listening on that port for the connection to succeed.

The following example overrides the default port.

```
switch# telnet 10.17.37.157 87
Trying 10.17.37.157...
Connected to 10.17.37.157.
Escape character is '^]'.
Network OS (sw0)
switch# login:
```

## Shutting down the Telnet service

Shutting down the Telnet service will forcibly disconnect all Telnet sessions running on a switch.

You must be in global configuration mode to shut down the Telnet service on a switch.

The Telnet service runs by default.

To shut down the Telnet service on a switch, enter **telnet server shutdown**.

```
switch(config)# telnet server shutdown
switch(config)#
```

All Telnet sessions are immediately terminated, and cannot be re-established until the service is re-enabled.

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# telnet server shutdown
```

## Re-enabling the Telnet service

Re-enabling the Telnet service permits Telnet access to a switch.

You must be in global configuration mode to shut down the Telnet service on a switch.

To re-enable the Telnet service on a switch enter **no telnet server shutdown**.

```
switch(config)# no telnet server shutdown
```

### NOTE

If you are in VCS mode, you must enter RBridge ID configuration mode before issuing the command.

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# no telnet server shutdown
```

## Connecting with SSH

Connecting to a switch using the SSH (Secure Socket Handling) protocol permits a secure (encrypted) connection.

For a listing and description of all configuration modes discussed here, refer to [Operational modes](#) on page 57.

## Establishing an SSH connection

An SSH (Secure Socket Handling) connection allows you to securely access a switch remotely.

You must be in privileged EXEC mode to make an SSH connection to a switch.

1. To establish an SSH connection with default parameters, enter **ssh -l** followed by the *username* you want to use and the *ip\_address* of the switch.

```
switch# ssh -l admin 10.20.51.68
```

2. Enter **yes** if prompted.

```
The authenticity of host '10.20.51.68 (10.20.51.68)' can't be established.
RSA key fingerprint is ea:32:38:f7:76:b7:7d:23:dd:a7:25:99:e7:50:87:d0.
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '10.20.51.68' (RSA) to the list of known hosts.
admin@10.20.51.68's password: *****
```

```
SECURITY WARNING: The default password for at least
one default account (root, admin and user) have not been changed.
Welcome to the Brocade Network Operating System Software
```

```
admin connected from 10.20.51.66 using ssh on C60_68F
```

#### NOTE

You can use the **-m** and **-c** options to override the default encryption and hash algorithms.

```
switch# ssh -l admin -m hmac-md5 -c aes128-cbc 10.20.51.68
```

## Importing an SSH public key

Importing an SSH public key allows you to establish an authenticated login for a switch.

You must be in privileged EXEC mode to import an SSH public key to a switch.

#### 1. NOTE

The following example allows you to import the SSH public key for the user "admin" from a remote host using the credentials shown.

To import an SSH public key, enter **certutil import sshkey**, followed by **user Username host IP\_Address directory File\_Path file Key\_filename login Login\_ID**.

```
switch# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/bmeenaks/.ssh file id_rsa.pub login fvt
```

#### 2. Enter the password for the user.

```
Password: *****
```

```
switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX6740-48, Event: sshutil, Status: success, Info: Imported SSH public key from 10.70.4.106 for user 'admin'.
```

#### NOTE

If you are in VCS mode, you must enter RBridge ID configuration mode before issuing the command.

```
switch# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/bmeenaks/.ssh file id_rsa.pub login fvt rbridge-id 3
```

## Deleting an SSH public key

Deleting an SSH public key from a switch prevents it from being used for an authenticated login.

You must be in privileged EXEC mode to delete an SSH public key from a switch.

To delete an SSH public key, enter **no certutil sshkey user Username** followed by either **rbridge-id rbridge-id** or **rbridge-id all**.

```
switch# no certutil sshkey user admin rbridge-id all
```

Specifying a specific RBridge ID removes the key from that RBridge ID; specifying all removes it from all RBridge IDs on the switch.

## Shutting down the SSH service

Shutting down the SSH (Secure Socket Handling) service will forcibly disconnect all SSH sessions running on a switch.

You must be in global configuration mode to shut down the SSH service on a switch.

The SSH service runs by default.

To shut down the SSH service on a switch, enter **ssh server shutdown**.

```
switch(config)# ssh server shutdown
switch(config)#
```

All SSH sessions are immediately terminated, and cannot be re-established until the service is re-enabled.

#### NOTE

If you are in VCS mode, you must enter RBridge ID configuration mode before issuing the command.

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# ssh server shutdown
switch(config-rbridge-id-3)#
```

## Re-enabling the SSH service

Re-enabling the SSH (Secure Socket Handling) service permits SSH access to a switch.

You must be in global configuration mode to shut down the SSH service on a switch.

To re-enable the SSH service on a switch enter **no ssh server shutdown**.

```
switch(config)# no ssh server shutdown
switch(config)#
```

#### NOTE

If you are in VCS mode, you must enter RBridge ID configuration mode before issuing the command.

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# no ssh server shutdown
```

## Using the management VRF

Virtual Routing and Forwarding (VRF) is a technology that controls information flow within a network, isolating the traffic by partitioning the network into different logical VRF domains. Prior to Network OS release 5.0.0, routers were managed through the "default" VRF; any port that was part of the default VRF could be used for router management.

## Configuring and managing switches

The following sections describe how to configure and manage Brocade switches.

### Configuring Ethernet management interfaces

The Ethernet network interface provides management access, including direct access to the Network OS CLI. You must configure at least one IP address using a serial connection to the CLI before you can manage the system with other management interfaces. You can either configure static IP addresses, or you can use a Dynamic Host Configuration Protocol (DHCP) client to acquire IP addresses automatically. For IPv6 addresses, both static IPv6 and stateless IPv6 autoconfiguration are supported.

#### ATTENTION

Setting static IPv4 addresses and using DHCP are mutually exclusive. If DHCP is enabled, remove the DHCP client before you configure a static IPv4 address. However, this does not apply to IPv6 addresses.

#### NOTE

You must connect through the serial port to set the IP address if the network interface is not configured already. Refer to the *Brocade VDX Hardware Reference* manual for your specific product for information on connecting through the serial port.

## Configuring static IP addresses

Use static Ethernet network interface addresses in environments where the DHCP service is not available. To configure a static IPv4 or IPv6 address, you must first disable DHCP. Refer to [Configuring IPv4 and IPv6 addresses with DHCP](#) on page 70 for more information.

### Configuring a static IPv4 Ethernet address

1. Connect to the switch through the serial console.
2. In privileged EXEC mode, issue the **configure terminal** command to enter global configuration mode.
3. Enter the **interface management** *rbridge-id/port* command to configure the management port.

This command enters a management interface configuration mode where you can choose configuration parameters for IPv4 and IPv6 addresses.

- A Top-of-Rack (ToR) switch has a single management port, and the port number for the management port is always 0.
- On a modular switch with two redundant management modules, you can configure two management ports. The port numbers are 1 and 2.

4. Enter the **no ip address dhcp** command to disable DHCP.
5. Enter the **ip address** *IPv4\_address/prefix\_length* command.
6. Configure an IPv4 management VRF with a default gateway address.

```
device(config-rbridge-id-1)# vrf mgmt-vrf
device(config-vrf-mgmt-vrf)# address-family ipv4 unicast
device(vrf-ipv4-unicast)# ip route 0.0.0.0/0 <default-gateway-ipv4-addr>
device(vrf-ipv4-unicast)# exit
device(config-vrf-mgmt-vrf)# exit
device#(config)# copy running-config startup-config
```

7. Verify the configuration with the **do show running-config interface management** command.

#### NOTE

Specifying an IPv4 address with a subnet mask is not supported. Instead, enter a prefix number in Classless Inter-Domain Routing (CIDR) notation. To enter a prefix number for a network mask, type a forward slash (/) and the number of bits in the mask immediately after the IP address. For example, enter, "209.157.22.99/24" for an IP address that has a network mask with 24 leading 1s in the network mask, representing 255.255.255.0.

```
switch(config-Management-1/0)# do show running-config interface management
interface Management 1/0
no ip address dhcp
ip address 10.24.85.81/20
vrf forwarding mgmt-vrf
no ipv6 address autoconfig
```

8. Apart from the two IP addresses on the management modules, modular switches also supports a chassis virtual IP address. Using this virtual IP address, you can login to the switch. The VCS virtual IP address binds to the active MM automatically.

```
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)# chassis virtual-ip 10.24.85.90/20
```

#### NOTE

In DHCP mode, the chassis IP address is obtained by means of DHCP.

### Configuring a static IPv6 Ethernet address

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.

2. Enter the **interface management** *rbridge-id/port* command.

This command enters a management interface configuration mode where you can choose configuration parameters for IPv4 and IPv6 addresses.

- A Top-of-Rack (ToR) switch has a single management port, and the port number for the management port is always 0.
- On a modular switches with two redundant management modules, you can configure two management ports. The port numbers are 1 and 2.

3. Enter the **IPv6 address** *IPv6\_address/prefix\_length* command.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface management 1/0
switch(config-Management-1/0)# ipv6 address fd00:60:69bc:832:e61f:13ff:fe67:4b94/64
```

4. Configure an IPv6 management VRF with a default gateway address.

```
device(config-rbridge-id-1)# vrf mgmt-vrf
device(config-vrf-mgmt-vrf)# address-family ipv6 unicast
device(vrf-ipv4-unicast)# ip route 0:0:0:0:0:0:0/0 <default-gateway-ipv6-addr>
device(vrf-ipv4-unicast)# exit
device(config-vrf-mgmt-vrf)# exit
device#(config)# copy running-config startup-config
```

5. Apart from the two IP addresses on the management modules, modular switches also support a chassis virtual IP address. Using this virtual IP address, you can log in to the switch. The VCS virtual IP address binds to the active MM automatically.

```
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)# chassis virtual-ipv6 2001:db8:8086:6502/64
```

## Configuring IPv4 and IPv6 addresses with DHCP

By default, DHCP is disabled. You must explicitly enable the service. Use the **ip address dhcp** command to enable DHCP for IPv4 addresses, and the **ipv6 address dhcp** command to enable DHCP for IPv6 addresses. The Network OS DHCP clients support the following parameters:

- External Ethernet port IP addresses and prefix length
- Default gateway IP address

### NOTE

When you connect the DHCP-enabled switch to the network and power on the switch, the switch automatically obtains the Ethernet IP address, prefix length, and default gateway address from the DHCP server. The DHCP client can only connect to a DHCP server on the same subnet as the switch. Do not enable DHCP if the DHCP server is not on the same subnet as the switch.

The following example enables DHCP for IPv4 addresses.

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

The following example enables DHCP for IPv6 addresses.

```
switch(config)# interface management 1/1
switch(config-Management-1/1)# ipv6 address dhcp
```

The **show running-config interface management** command indicates whether DHCP is enabled. The following example shows a switch with DHCP enabled for IPv4 addresses.

```
switch# show running-config interface management
interface Management 2/0
ip address dhcp
ip route 0.0.0.0/0 10.24.80.1
ip address 10.24.73.170/20
no ipv6 address autoconfig
```

#### NOTE

Enabling DHCP removes all configured static IP addresses.

#### NOTE

Refer to the Network OS Layer 3 Routing Configuration Guide for more information on configuring IP DHCP relay.

## Configuring IPv6 autoconfiguration

Refer also to [Stateless IPv6 autoconfiguration](#) on page 56.

1. In privileged EXEC mode, issue the **configure terminal** command to enter global configuration mode.
2. Take the appropriate action based on whether you want to enable or disable IPv6 autoconfiguration.
  - Enter the **ipv6 address autoconfig** command to enable IPv6 autoconfiguration for all managed entities on the target platform.
  - Enter the **no ipv6 address autoconfig** command to disable IPv6 autoconfiguration for all managed entities on the target platform.

#### NOTE

On the Brocade VDX 8770, the **autoconfig** command can be issued only on the interface *rbridge-id/1*. However, this operation enables auto-configuration for the entire chassis.

## Displaying the network interface

If an IP address has not been assigned to the network interface, you must connect to the Network OS CLI using a console session on the serial port. Otherwise, connect to the switch through Telnet or SSH. Enter the **show interface management** command to display the management interface.

The following example shows the management interface on a Brocade VDX Top-of-Rack (ToR) switch.

```
switch# show interface management
interface Management 9/0
ip address 10.24.81.65/20
ip gateway-address 10.24.80.1
ipv6 ipv6-address [ ]
ipv6 ipv6-gateways [ fe80::21b:edff:fe0f:bc00 fe80::21b:edff:fe0c:c200 ]
line-speed actual "1000baseT, Duplex: Full"
line-speed configured Auto
```

The following example shows the management interfaces on a Brocade VDX 8770-4. IPv6 autoconfiguration is enabled for the entire chassis, and, as a result, a stateless IPv6 address is assigned to both management interfaces.

```
switch# show interface management
interface Management 110/1
ip address 10.20.238.108/21
ip gateway-address 10.24.80.1
ipv6 ipv6-address [ "stateless fd00:60:69bc:85:205:33ff:fe78:7d88/64 preferred" ]
ipv6 ipv6-gateways [ fe80::21b:edff:fe0b:7800 fe80::21b:edff:fe0b:2400 ]
line-speed actual "1000baseT, Duplex: Full"
line-speed configured Auto
interface Management 110/2
```

```
ip address 10.20.238.109/21
ip gateway-address 10.24.80.1
ipv6 ipv6-address [ "stateless fd00:60:69bc:85:205:33ff:fe78:be14/64 preferred" ]
ipv6 ipv6-gateways [ fe80::21b:edff:fe0b:7800 fe80::21b:edff:fe0b:2400 ]
line-speed actual "1000baseT, Duplex: Full"
line-speed configured Auto
```

## Configuring the management interface speed

By default, the speed of the interface is set to autoconfiguration, which means the interface speed is optimized dynamically depending on load and other factors. You can override the default with a fixed speed value of 10 Mbps full duplex or 100 Mbps full duplex.

1. In privileged EXEC mode, issue the **configure terminal** command to enter global configuration mode.

```
switch# configure terminal
Entering configuration mode terminal
```

2. Enter the **interface management** command followed by *rbridge-id/O*.

This command places you in the management interface subconfiguration mode.

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

3. Enter the **speed** command with the selected speed parameter. The valid values are **10**, **100**, and **auto**.

```
switch(config-Management-1/0)# speed auto
```

4. Enter the **do show interface management** command followed by *rbridge-id/O* to display the new settings.

```
switch(config-Management-1/0)# do show interface management 1/0
interface Management 1/0
ip address 10.24.81.65/20
ip route 0.0.0.0/0 10.24.80.1
ipv6 ipv6-address [ ]
ipv6 ipv6-gateways [fe80::21b:edff:fe0f:bc00 fe80::21b:edff:fe0c:c200]
line-speed actual "1000baseT, Duplex: Full"
line-speed configured Auto
```

5. Save the configuration changes by using the **copy running-config startup-config** command.

```
switch(config-Management-1/0)# do copy running-config startup-config
```

## Configuring a switch banner

A banner is a text message that displays on the switch console. It can contain information about the switch that an administrator may want users to know when accessing the switch.

The banner can be up to 2048 characters long. To create a multi-line banner, enter the **banner login** command followed by the **Esc-m** keys. Enter **Ctrl-D** to terminate the input.

If you are in logical chassis cluster mode, the configuration is applied to all nodes in the cluster.

Complete the following steps to set and display a banner.

1. In privileged EXEC mode, issue the **configure terminal** command to enter global configuration mode.
2. Enter the **banner login** command and a text message enclosed in double quotation marks (" ").
3. Enter the **do show running-config banner** command to display the configured banner.

```
switch# configure terminal
Entering configuration mode terminal
```



```
switch(config)# banner login "Please do not disturb the setup on this switch"
switch(config)# do show running-config banner
banner login "Please do not disturb the setup on this switch"
```

Use the **no banner login** command to remove the banner.

## Configuring switch attributes

Refer also to:

- [Switch attributes](#) on page 56.
- [Switch types](#) on page 56.

## Setting and displaying the host name

1. In privileged EXEC mode, issue the **configure terminal** command to enter global configuration mode.
2. If Telnet is not activated on the switch, enter the **no telnet server disable** command to activate Telnet.
3. Enter the **switch-attributes** command, followed by a question mark (?) to determine the local RBridge ID.
4. Enter the **switch-attributes** command, followed by the RBridge ID.
5. Enter the **host-name** operand, followed by the host name.
6. Save the configuration changes by using the **do copy running-config startup-config** command.

### NOTE

This step is used for switches in fabric cluster mode only. If you are using logical chassis cluster mode, startup configurations are not maintained by the cluster; each node preserves its running configuration. For more information about logical chassis cluster mode, refer to [Logical chassis cluster mode](#) on page 58.

7. Verify the configuration with the **do show running-config switch-attributes rbridge-id** command.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no telnet server disable
switch(config)# switch-attributes ?
Possible completions: <NUMBER:1-239> Specify the rbridge-id 1
switch(config)# switch-attributes 1
switch(config-switch-attributes-1)# host-name lab1_vdx0023
switch(config-switch-attributes-1)# exit
switch(config)# do copy running-config startup-config
switch(config)# do show running-config switch-attributes 1
switch-attributes 1
chassis-name VDX 6740-48
host-name lab1_vdx0023
```

## Setting and displaying the chassis name

1. In privileged EXEC mode, issue the **configure terminal** command to enter global configuration mode.
2. Enter the **switch-attributes** command, followed by a question mark (?) to determine the local RBridge ID.
3. Enter the **switch-attributes** command, followed by the RBridge ID.
4. Enter the **chassis-name** operand, followed by the chassis name.
5. Save the configuration changes using the **do copy running-config startup-config** command.

**NOTE**

This step is used for switches in fabric cluster mode only. If you are using logical chassis cluster mode, startup configurations are not maintained by the cluster; each node preserves its running configuration. For more information about logical chassis cluster mode, refer to [Logical chassis cluster mode](#) on page 58.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# switch-attributes ?
Possible completions: <NUMBER:1-239> Specify the rbridge-id 1
switch(config)# switch-attributes 1
switch(config-switch-attributes-1# chassis-name lab1_vdx0023
switch(config)# do copy running-config startup-config
switch(config)# do show running-config switch-attributes 1
switch-attributes 1
  chassis-name lab1_vdx0023
  host-name lab1_vdx0023
```

**Viewing switch types**

The switchType attribute is a unique device model identifier that allows you to identify the model of a switch from the command line.

In this example, the number 1000 is the value of the switchType attribute. An optional number (.x) indicates the revision of the motherboard.

Refer also to [Switch types](#) on page 56.

Enter **show chassis**.

```
switch# show chassis
Chassis Family: VDX 87xx
Chassis Backplane Revision: 1
switchType: 1000 <== Use table to convert this parameter
(output truncated)
```

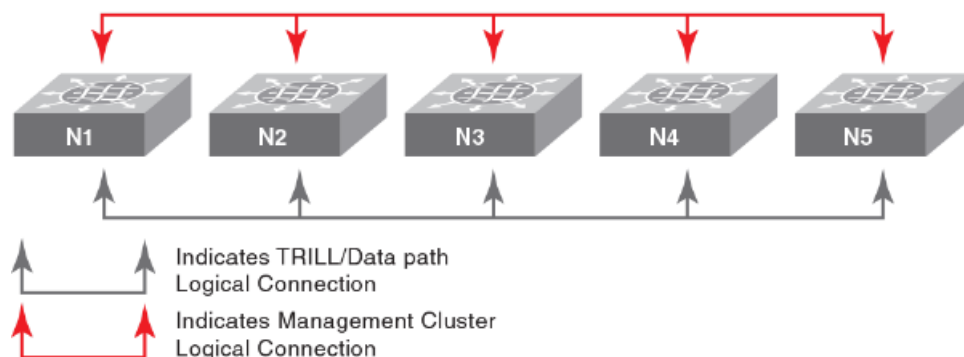
**Configuring a switch in logical chassis cluster mode**

Refer to [Logical chassis cluster mode](#) on page 58.

**Creating a logical chassis cluster**

This section covers the basic steps to create a logical chassis cluster, with the assumption that all physical connectivity requirements have been met. The following figure is a representation of a five-node logical chassis cluster.

FIGURE 13 Five-node logical chassis cluster



To create a logical chassis cluster, follow the steps in the following example:

1. Log in to one switch that will be a member of the logical chassis cluster you are creating:
2. In privileged EXEC mode, enter the **vcs** command with options to set the VCD ID, the RBridge ID and enable logical chassis mode for the switch. The VCS ID and RBridge IDs shown are chosen for the purposes of this example.

```
switch# vcs vcsid 22 rbridge-id 15 logical-chassis enable
```

3. The switch reboots after you run the **vcs** command. You are asked if you want to apply the default configuration; answer **yes**.
4. Repeat the previous steps for each node in the cluster, changing only the RBridge ID each time. You must, however, set the VCS ID to the same value on each node that belongs to the cluster.
5. When you have enabled the logical chassis mode on each node in the cluster, run the **show vcs** command to determine which node has been assigned as the cluster principal node. The arrow (>) denotes the principal node. The asterisk (\*) denotes the current logged-in node.

```
switch# show vcs
Config Mode      : Distributed
VCS Mode         : Logical Chassis
VCS ID           : 44
VCS GUID         : bcab366e-6431-42fe-9af1-c69eb67eaa28
Total Number of Nodes      : 3
Rbridge-Id       WWN                Management IP   VCS Status     Fabric Status   HostName
-----
144              10:00:00:27:F8:1E:3C:8C           10.18.245.143  Offline        Unknown        sw0
152              >10:00:00:05:33:E5:D1:93*         10.18.245.152  Online         Online         cz41-h06-
m-r2
158              10:00:00:27:F8:F9:63:41           10.18.245.158  Offline        Unknown
```

The RBridge ID with the arrow pointing to the WWN is the cluster principal. In this example, RBridge ID 154 is the principal.

6. Set the clock and time zone for the principal node. Time should be consistent across all the nodes. Refer to [Network Time Protocol overview](#) on page 111.
7. Log in to the principal cluster and make any desired global and local configuration changes. These changes then are distributed automatically to all nodes in the logical chassis cluster.

#### NOTE

You can enter the RBridge ID configuration mode for any RBridge in the cluster from the cluster principal node. You can change the principal node by using the **logical-chassis principal priority** and **logical chassis principal switchover** commands. For more information about cluster principal nodes, refer to [Selecting a principal node for the cluster](#) on page 79.

## Taking precautions for mode transitions

Ensure that all nodes to be transitioned are running the same version of Network OS. Logical chassis cluster mode is supported starting with Network OS release 4.0.0

If you are merging multiple global configuration files to create one new global configuration file, be sure that the same entity name does not exist in the merged file. For example, if mac access-list extended **test1** contains the entries shown in the following "Node 1 global configuration" and "Node 2 global configuration", when you merge the files you can rename mac access-list extended **test1** from Node 2 to mac access-list extended **test2**, as shown in the "Combined global configuration."

### Node 1 global configuration

```
mac access-list extended test1
seq 10 permit any 1111.2222.333a ffff.ffff.ffff
seq 20 deny any 1111.2222.333b ffff.ffff.ffff
```

```
seq 30 deny any 1111.2222.333c ffff.ffff.ffff
seq 40 permit any any
```

### Node 2 global configuration

```
mac access-list extended test1
seq 10 permit any 4444.5555.666d ffff.ffff.ffff
seq 20 deny any 4444.5555.666e ffff.ffff.ffff
seq 30 permit any any
```

### Combined global configuration

```
mac access-list extended test1
seq 10 permit any 1111.2222.333a ffff.ffff.ffff
seq 20 deny any 1111.2222.333b ffff.ffff.ffff
seq 30 deny any 1111.2222.333c ffff.ffff.ffff
seq 40 permit any any
!
mac access-list extended test2
seq 10 permit any 4444.5555.666d ffff.ffff.ffff
seq 20 deny any 4444.5555.666e ffff.ffff.ffff
seq 30 permit any any
```

The local configuration for Node 2 also needs to be changed accordingly. In this example, one of the local configuration changes would be the interface TenGigabitEthernet. Instead of referencing **test1**, the local configuration file for Node 2 needs to reference **test2** because of the change that was made to the global configuration file. This is shown in the following "Node 2 local configuration..." sections.

### Node 2 local configuration *before* matching the combined global configuration

```
interface TenGigabitEthernet 4/0/3
fabric isl enable
fabric trunk enable
switchport
switchport mode access
switchport access vlan 1
spanning-tree shutdown
mac access-group test1 in
no shutdown
```

### Node 2 local configuration *after* matching the combined global configuration

```
interface TenGigabitEthernet 4/0/3
fabric isl enable
fabric trunk enable
switchport
switchport mode access
switchport access vlan 1
spanning-tree shutdown
mac access-group test2 in
no shutdown
```

#### ATTENTION

Be sure to take the following precautions.

- Note that the **copy default-config to startup-config** command in logical chassis cluster mode causes a cluster-wide reboot and returns the entire logical chassis cluster to the default configuration. Therefore, use this command only if you want to purge all existing configuration in the logical chassis cluster.
- Make sure that the backup files for global and local configurations are available in a proper SCP or FTP location that can be easily retrieved in logical chassis cluster mode during restore. Do not save the files in the local flash, because they may not be available on the principal node for replay of local configurations.

## Converting a fabric cluster to a logical chassis cluster

You can convert an existing fabric cluster to a logical chassis cluster using the default configuration file.

1. Be sure all nodes are running the same firmware version. Logical chassis cluster functionality is supported in Network OS 4.0.0 and later.
2. Be sure all the nodes that you intend to transition from a fabric cluster to a logical chassis cluster are online. Run either the **show vcs** or **show vcs detail** command to check the status of the nodes.
3. Log in to one switch that you are converting from fabric cluster mode to logical chassis cluster mode.
4. In Privileged EXEC mode, enter the **vcs logical-chassis enable** command with desired options; for example you can convert all R Bridges with one command:

```
switch# vcs logical-chassis enable rbridge-id all default-config
```

### NOTE

To convert a specific R Bridge from fabric cluster mode to logical chassis mode, use the R Bridge ID value in place of the "all" option. You can also specify a range, such as "1,3,4-6". Refer to the *Network OS Command Reference* for details.

The nodes automatically reboot in logical chassis cluster mode. Allow for some down time during the mode transition.

5. Run either the **show vcs** or the **show vcs detail** command to check that all nodes are online and now in logical chassis cluster (listed as "Distributed" in the command output) mode.
6. The **show vcs** command output can also be used to determine which node has been assigned as the cluster principal node.

```
switch# show vcs
R-Bridge      WWN                               Switch-MAC          Status
-----
1      > 11:22:33:44:55:66:77:81      AA:BB:CC::DD:EE:F1  Online
2      11:22:33:44:55:66:77:82      AA:BB:CC::DD:EE:F2  Online
3      11:22:33:44:55:66:77:83*      AA:BB:CC::DD:EE:F3  Online
```

The R Bridge ID with the arrow pointing to the WWN is the cluster principal. In this example, R Bridge ID 1 is the principal.

7. Log in to the principal cluster and make any desired global and local configuration changes. These changes then are distributed automatically to all nodes in the logical chassis cluster.

### NOTE

You can enter the R Bridge ID configuration mode for any R Bridge in the cluster from the cluster principal node.

### NOTE

You can change the principal node by using the **logical-chassis principal priority** and **logical chassis principal switchover** commands. For more information about cluster principal nodes, refer to [Selecting a principal node for the cluster](#) on page 79.

## Converting a fabric cluster while preserving configuration

There is no specific command that can convert a fabric cluster to a logical chassis cluster while preserving current configurations, but you can accomplish this task as follows:

1. Be sure that all nodes are running the same firmware version. Logical chassis cluster functionality is supported in Network OS 4.0 and later.
2. Make sure all the nodes that you intend to transition from a fabric cluster to a logical chassis cluster are online. Run either the **show vcs** or **show vcs detail** command to check the status of the nodes.

- Determine which node contains the global configuration you want to use on the logical chassis cluster, and make a backup of this configuration by running the **copy global-running-config** command and saving the configuration to a file on a remote FTP, SCP, SFTP, or USB location:

**NOTE**

If you need to combine the global configurations of two or more nodes, manually combine the required files into a single file which will be replayed after the transition to logical chassis cluster mode by using the **copy global-running-config** *location\_config\_filename* command. Refer to the section [Taking precautions for mode transitions](#) on page 75

- Back up the local configurations of all individual nodes in the cluster, by running the **copy local-running-config** command on each node and saving the configuration to a file on a remote ftp, scp, sftp, or usb location:

**copy local-running-config** *location\_config\_filename*

- Perform the mode transition from fabric cluster to logical chassis cluster by running the **vcs logical-chassis enable rbridge-id all default-config** command, as shown in [Converting a fabric cluster to a logical chassis cluster](#) on page 77.

The nodes automatically reboot in logical chassis cluster mode. Allow for some down time during the mode transition.

- Run either the **show vcs** or the **show vcs detail** command to check that all nodes are online and now in logical chassis cluster (listed as "Distributed" in the command output) mode.
- The **show vcs** command output can also be used to determine which node has been assigned as the cluster principal node.

```
switch# show vcs
R-Bridge      WWN                               Switch-MAC          Status
-----
1      >  11:22:33:44:55:66:77:81          AA:BB:CC::DD:EE:F1  Online
2      11:22:33:44:55:66:77:82          AA:BB:CC::DD:EE:F2  Online
3      11:22:33:44:55:66:77:83*        AA:BB:CC::DD:EE:F3  Online
```

The RBridge ID with the arrow pointing to the WWN is the cluster principal. In this example, RBridge ID 1 is the principal.

- While logged on to the principal node in the logical chassis cluster, copy the saved global configuration file from the remote location to the principal node as follows:

**copy** *location\_config\_filename* **running-config**

- Verify that the global configuration is available by running the **show global-running-config** command.
- While logged on to the principal node in the logical chassis cluster, copy each saved local configuration file from the remote location to the principal node as follows:

**copy** *location\_config\_filename* **running-config**

**NOTE**

You must run this command for each local configuration file you saved (one for each node).

The configuration file is automatically distributed to all nodes in the logical chassis cluster. Each node will contain the same global configuration after the previous steps are performed. Each node will also contain the local configuration information of all the other nodes.

- Verify that the local configurations are available by running the **show local-running-config** command.
- Log in to the principal cluster and make any desired global and local configuration changes. These changes then are distributed automatically to all nodes in the logical chassis cluster.

**NOTE**

You can enter the RBridge ID configuration mode for any RBridge in the cluster from the cluster principal node. You can change the principal node by using the **logical-chassis principal priority** and **logical chassis principal switchover** commands. For more information about cluster principal nodes, refer to [Selecting a principal node for the cluster](#) on page 79.

## Selecting a principal node for the cluster

Logical chassis cluster principal node behavior includes:

- All configuration for the logical chassis cluster must be performed on the principal node.
- By default, the node with the lowest WWN number becomes the principal node.
- You can run the **show vcs** command to determine which node is the principal node. An arrow in the display from this command points to the WWN of the principal node.
- You can select any node in the logical chassis cluster to become the principal by running the **logical chassis principal priority** command, followed by the **logical-chassis principal switchover** command, as shown in the following example (in this example, RBridge ID 5 is being assigned with the highest priority):

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# logical-chassis principal-priority 1
switch(config-rbridge-id-5)# end
switch# logical-chassis principal-switchover
```

A lower number means a higher priority. Values range from 1 to 128.

Until you run the **logical-chassis principal switchover** command, the election of the new principal node does not take effect.

## Converting a logical chassis cluster to a fabric cluster

To transition all nodes in a logical chassis cluster to a fabric cluster, using default configurations, perform these steps:

1. Make sure all the nodes that you intend to transition from a logical chassis cluster to a fabric cluster are online. Run either the **show vcs** or **show vcs detail** command to check the status of the nodes.
2. Log in to the principal node on the logical chassis cluster.
3. Run the following command to convert all RBridge IDs: **no vcs logical-chassis enable rbridge-id all default-config**.

### NOTE

To convert just one RBridge ID, specify the ID as shown in the following example: **no vcs logical-chassis enable rbridge-id rbridge-id default-config**.

The nodes automatically reboot in fabric cluster mode. Plan for some down time for this transition.

4. Run either the **show vcs** or **show vcs detail** command to check that all nodes are online and now in fabric cluster (listed as "Local-only" in the command output) mode.

## Converting to a fabric cluster while preserving configuration

There is no specific command that can convert a logical chassis cluster to a fabric cluster while preserving current configurations, but you can accomplish this task as follows:

1. Make sure all the nodes that you intend to transition from a logical chassis cluster to a fabric cluster are online. Run either the **show vcs** or **show vcs detail** command to check the status of the nodes.
2. Back up the configurations of all nodes in the cluster by running the **copy rbridge-running-config rbridge-id** command on each node and saving the configuration to a file on a remote FTP, SCP, SFTP, or USB location:

```
copy rbridge-running-config rbridge-id rbridge-id location_configfilename
```

This command copies both the global and local configurations for the specified RBridge ID.

3. From the principal node of the logical chassis cluster, transition the entire cluster to fabric cluster mode (using the default configuration) by running the following command:

```
no vcs logical-chassis enable rbridge-id all default-config
```

The nodes automatically reboot in fabric cluster mode. Plan for some down time for this transition.

- Run either the **show vcs** or **show vcs detail** command to check that all nodes are online and now in fabric cluster (listed as "Local-only" in the command output) mode.
- Restore the global and local configurations on each individual node for which you backed up these configurations by running the following command on each node:

```
copy location_configfilename running-config
```

- To cause this downloaded configuration to be persistent for a node, run the **copy running-config startup-config** command.

### Adding a node to a logical chassis cluster

Nodes can be dynamically added to an existing logical chassis cluster. If the proper physical connections exist between the existing logical chassis cluster and the new node, the process is automatic.

Log into the new node and run the **vcs logical-chassis enable** command with the desired options. You must assign the new node the VCS ID of the existing cluster.

You can run the **show vcs** command to verify that the status of the added node is "online."

### Removing a node from a logical chassis cluster

If the **no vcs logical-chassis enable rbridge-id <rbridge-id / all> default-config** command is executed on a switch that is currently in logical chassis cluster mode, the switch boots in fabric cluster mode. The following is example:

```
no vcs logical-chassis enable rbridge-id 239 default-config
```

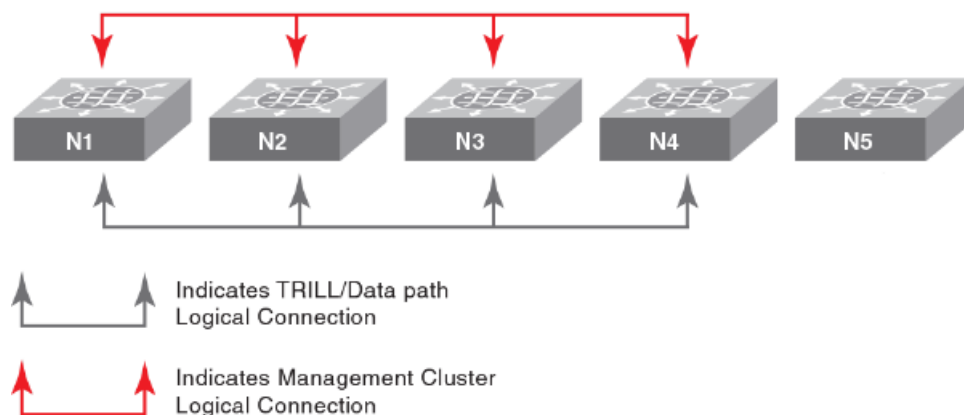
Once the node is converted to fabric cluster mode, the Rbridge goes into offline state from the original cluster. To remove the configuration of the node, you must enter the **no vcs enable rbridge-id rbridge-id** command, as shown in the following example:

```
no vcs enable rbridge-id 239
```

Once the node is removed, all configurations corresponding to that node are removed from the cluster configuration database. Similarly, the removed node does not retain any configurations corresponding to the other nodes in the cluster.

The following figure shows the cluster after node N5 has been removed. Nodes N1 through N4 remain in the cluster, and N5 is an island. There is no data path or management path connectivity between the two islands.

FIGURE 14 Removal of Node N5 from the logical chassis cluster





## Rejoining a node to the cluster

Nodes that are temporarily isolated from a logical chassis cluster can re-join the cluster as long as no configuration or cluster membership changes have taken place on either the deleted node or the cluster. Run the **vcs logical-chassis enable** command with the desired options to rejoin the node to the cluster.

However, if configuration changes have occurred on either the node or cluster since the node was removed, you must reboot the node with its default configuration by issuing **copy default-config startup-config** on the segmented node.

## Replacing a node in a logical chassis cluster

If a node in a logical chassis cluster becomes damaged and can no longer be used, a similar node with identical capabilities can be used in its place.

The new node must use the same RBridge ID of the node that is being replaced. When the new node is detected, it joins the cluster as a previously known node instead of being considered a new node.

In the following VDX fabric example of four switches, RBridge-ID 2 is considered to be faulty and must be replaced:

```
device# show vcs
Config Mode      : Distributed
VCS Mode         : Logical Chassis
VCS ID           : 10
VCS GUID         : bd9870ed-3309-4839-bda5-ac179603662c
Total Number of Nodes      : 4
Rbridge-Id      WWN                Management IP    VCS Status    Fabric Status    HostName
-----
1                >10:00:00:05:33:40:32:93*  10.17.76.74     Online        Online          VDX1-6720
2                10:00:00:05:33:7D:6C:E6   10.17.76.76     Online        Online          VDX2-6730
3                10:00:00:27:F8:17:C6:A8   10.17.76.121    Online        Online          VDX3-8770
4                10:00:00:05:33:AC:AF:DB   10.17.76.72     Online        Online          VDX4-6710
```

1. Upgrade the new device to the same firmware version as the rest of the logical chassis cluster. The new device should be the same model and configuration as the device being replaced.
2. Configure the same VCS ID, Rbridge-ID, and logical chassis mode on the new device as the rest of the logical chassis cluster. If properly done, the device automatically reboots. For this example, the command would be as follows.

```
device# vcs vcsid 10 rbridge-id 2 logical-chassis enable
```

3. Once the new device reboots, run the **show vcs** command on the new device and make note of the WWN ID of the new device.

```
device# show vcs
Config Mode      : Distributed
VCS ID           : 10
VCS GUID         : 00000000000000000000000000000000
Total Number of Nodes      : 1
Rbridge-Id      WWN                Management IP    VCS Status    Fabric Status    HostName
-----
2                >10:00:00:05:33:7D:76:B0*  10.17.76.91     Online        Online          sw0
```

4. Disconnect all data cables from the faulty device to be replaced. Make notes of the cable connections.
5. The **show vcs** command displays the RBridge ID as being offline.

```
device# show vcs
Config Mode      : Distributed
VCS Mode         : Logical Chassis
VCS ID           : 10
VCS GUID         : bd9870ed-3309-4839-bda5-ac179603662c
Total Number of Nodes      : 4
Rbridge-Id      WWN                Management IP    VCS Status    Fabric Status    HostName
-----
1                >10:00:00:05:33:40:32:93*  10.17.76.74     Online        Online          VDX1-6720
2                10:00:00:05:33:7D:6C:E6   10.17.76.76     Offline       Unknown         sw0
```

```

3          10:00:00:27:F8:17:C6:A8    10.17.76.121    Online          Online          VDX3-8770
4          10:00:00:05:33:AC:AF:DB    10.17.76.72     Online          Online          VDX4-6710

```

- On the principal device of the Logical Chassis cluster, enter the **vcs replace** command for the RBridge-ID of the replaced device. The fabric will prompt for the WWN ID of the new switch.

```

device# vcs replace rbridge-id 2
Enter the WWN of the new replacement switch:10:00:00:05:33:7D:76:B0
This operation will remove and replace the switch from the fabric. Do you want to continue? [Y/N] y

```

- The **show vcs** command displays the RBridge ID as being replaced.

```

device# show vcs
Config Mode      : Distributed
VCS Mode         : Logical Chassis
VCS ID           : 10
VCS GUID         : bd9870ed-3309-4839-bda5-ac179603662c
Total Number of Nodes      : 4
Rbridge-Id       WWN          Management IP   VCS Status     Fabric Status   HostName
-----
1          >10:00:00:05:33:40:32:93*  10.17.76.74    Online          Online          VDX1-6720
2          10:00:00:05:33:7D:76:B0     10.17.76.76    Replacing      Online          VDX2-6730
3          10:00:00:27:F8:17:C6:A8     10.17.76.121   Online          Online          VDX3-8770
4          10:00:00:05:33:AC:AF:DB     10.17.76.72    Online          Online          VDX4-6710

```

- Add the new switch hardware to the network and connect all data cables.
- Once the ISL interfaces boot, the **show vcs** command status changes from Rejoining to Online.

```

device# show vcs
Config Mode      : Distributed
VCS Mode         : Logical Chassis
VCS ID           : 10
VCS GUID         : bd9870ed-3309-4839-bda5-ac179603662c
Total Number of Nodes      : 4
Rbridge-Id       WWN          Management IP   VCS Status     Fabric Status   HostName
-----
1          >10:00:00:05:33:40:32:93*  10.17.76.74    Online          Online          VDX1-6720
2          10:00:00:05:33:7D:76:B0     10.17.76.76    Rejoining      Online          VDX2-6730
3          10:00:00:27:F8:17:C6:A8     10.17.76.121   Online          Online          VDX3-8770
4          10:00:00:05:33:AC:AF:DB     10.17.76.72    Online          Online          VDX4-6710

```

## Merging two logical chassis clusters

You can merge two logical chassis clusters that have the same VCS ID. Follow these steps:

- Make all required physical connections between the two independent clusters.
- Decide which cluster should retain the configuration after the merge. Only one configuration can be retained.
- On the cluster whose configuration will not be retained, issue the **copy default-config startup-config** command so that the nodes in this cluster will reboot with the default configuration.
- Reboot all nodes in each cluster. The logical chassis cluster whose configuration is being retained recognizes the nodes from the other cluster as new nodes and adds them accordingly.
- Re-apply the configuration to the cluster whose configuration was not retained.

## Changing an RBridge ID on a switch within a fabric

It may become necessary to change the RBridge ID number on a switch that rebooted and has become orphaned from the cluster.

- Backup the global configuration before changing the RBridge ID, because the local configuration will be reset to default values. Refer to [Backing up configurations](#) on page 118.

- On the rebooted switch, execute the **chassis disable** command.

```
switch# chassis disable
```

- From the fabric principal switch, execute the **no vcs enable rbridge-id rbridge-id** command, where *rbridge-id* is the switch that was orphaned.

```
switch# no vcs enable rbridge-id 3
```

- On the rebooted switch, execute the **vcs rbridge-id rbridge-id** command, where *rbridge-id* is the RBridge you want to use.
- The VCSID should already be set, if it's not set it with the **vcs rbridge-id rbridge-id**.
- Reboot the orphaned switch.

The following behavior will take effect after the switch reboots:

- All interfaces will be in *shutdown* state. You must perform a **no shutdown** command on ISL interfaces before the switch will rejoin the cluster.
  - The original configuration will be lost and the switch will have a default configuration when it rejoins the cluster with the new RBridge ID.
- Use the **show vcs detail** command to verify that the switch is in the fabric.

```
switch# show vcs detail
Config Mode : Local-Only
VCS ID : 1
Total Number of Nodes : 6
Node :1
Serial Number : BKN2501G00R
Condition : Good
Status : Connected to Cluster
VCS Id : 1
Rbridge-Id : 38
Co-ordinator : NO
WWN : 10:00:00:05:33:52:2A:82
Switch MAC : 00:05:33:52:2A:82
FCF MAC : 0B:20:B0:64:10:27
Switch Type : BR-VDX6720-24-C-24
Internal IP : 127.1.0.38
Management IP : 10.17.10.38
Node :2
Serial Number : BZA0330G00P
```

## Examples of global and local configurations

The following table provides examples of global and local configuration commands that are available under the respective configuration modes. These settings can be viewed respectively by means of the **show global-running-config** command and the **show local-running-config** command.

**TABLE 13** Global and local configuration commands

Global	Local
Interface vlan	switch-attributes
interface port-channel	interface management
port-profile	interface ve
mac access-list	diag post
ip access-list	dpod
sflow	switch-attributes
snmp-server	fabric route mcast

**TABLE 13** Global and local configuration commands (continued)

Global	Local
protocol lldp	rbridge-id
zoning	ip route
cee-map	linecard
username	router ospf
	ipv6 router ospf
	router bgp
	protocol vrrp
	vrrp-group
	interface management
	interface gigabitethernet
	interface tengigabitethernet
	interface fortygigabitethernet
interface fcoe	

Use the **copy snapshot** commands if you need to upload or download configuration snapshot files to and from an ftp or scp server. You may need to use these commands if you took a snapshot of a configuration on a node that was disconnected from the cluster.

Refer to the *Network OS Command Reference* for detailed information about these and other logical chassis server commands.

## Configuring a switch in fabric cluster mode

Refer also to [Fabric cluster mode \(VCS Fabrics only\)](#) on page 60. When you issue the **show vcs** command to display the VCS configuration for the chassis, the command output shows a single-node VCS with a VCS ID of 1 and an RBridge ID of 1. Use the **vcs** command to change the default values.

```
switch0# show vcs
Config Mode   : Local-Only
VCS ID       : 1
Total Number of Nodes : 1
Rbridge-Id WWN
-----
1             >10:00:00:05:33:51:63:42* 10.17.37.154 Online   Online   switch0
2607:f0d0:1002:ff51:ffff:ffff:ffff:fff5
```

## Displaying switch interfaces

Interfaces on the VDX 8770 platform are identified by the RBridge ID, slot number, and port number, separated by forward slashes (/). For example, the notation 9/2/8 indicates port 8 located in slot 2 on a chassis with the RBridge ID of 9.

Enter the **show running-config interface *interface\_type*** command to display the interfaces and their status.

```
switch# show running-config interface tengigabitethernet
interface tengigabitethernet 1/1/1
fabric isl enable
fabric trunk enable
no shutdown
!
interface tengigabitethernet 1/1/2
fabric isl enable
fabric trunk enable
no shutdown
!
interface tengigabitethernet 1/1/3
```

```

fabric isl enable
fabric trunk enable
no shutdown
!
interface tengigabitethernet 1/1/4
fabric isl enable
fabric trunk enable
no shutdown
!
interface tengigabitethernet 1/1/5
fabric isl enable
fabric trunk enable
no shutdown
!
interface tengigabitethernet 1/1/6
fabric isl enable
fabric trunk enable
no shutdown

```

Enter the **show interface** *interface\_type rbridge\_id/slot/port* command to display the configuration details for the specified interface.

```

switch# show interface tengigabitethernet 1/1/9
tengigabitethernet 1/1/9 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0005.3315.df5a
Current address is 0005.3315.df5a
Pluggable media present
Interface index (ifindex) is 4702109825
MTU 9216 bytes
LineSpeed Actual    : 10000 Mbit
LineSpeed Configured : Auto, Duplex: Full
Flowcontrol rx: off, tx: off
Priority Tag disable
Last clearing of show interface counters: 04:12:03
Queueing strategy: fifo
Receive Statistics:
1580 packets, 140248 bytes
Unicasts: 0, Multicasts: 1580, Broadcasts: 0
64-byte pkts: 0, Over 64-byte pkts: 1561, Over 127-byte pkts: 17
Over 255-byte pkts: 2, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
Over 1518-byte pkts(Jumbo): 0
Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
Errors: 0, Discards: 0, TrillportCtrlFrames: 1564
Transmit Statistics:
1583 packets, 140120 bytes
Unicasts: 0, Multicasts: 1583, Broadcasts: 0
Underruns: 0
Errors: 0, Discards: 0, TrillportCtrlFrames: 1583
Rate info:
Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:15:53

```

Refer also to [Slot numbering and configuration](#) on page 64.

## Displaying slots and module status information

Use the **show slots** command to display information for all slots in the chassis. The following example shows slot information for the Brocade VDX 8770-8.

```

switch# show slots
Slot  Type      Description                               ID      Status
-----
M1    MM           Management Module                         112     ENABLED
M2    MM           Management Module                         112     ENABLED
S1    SFM          Switch Fabric Module                      113     ENABLED
S2                                VACANT@
S3    SFM          Switch Fabric Module                      113     ENABLED#
S4    SFM          Switch Fabric Module                      113     ENABLED#
S5    SFM          Switch Fabric Module                      113     ENABLED

```

```

S6   SFM           Switch Fabric Module       113   ENABLED
L1                                     VACANT
L2                                     VACANT
L3   LC48X10G     48-port 10GE card       114   DIAG RUNNING POST1
L4   LC48X10G     48-port 10GE card       114   ENABLED
L5                                     VACANT
L6                                     VACANT
L7   LC48X1G      48-port 1GE card        114   ENABLED
L7                                     VACANT
L8                                     VACANT
# = At least one enabled SFM in these slots is required.
@ = The SFM Optical Switch is open.

```

Alternatively, you can use the following commands to display slots per module type:

- Use the **show mm** command to display information for the management modules.
- Use the **show sfm** command to display information for the switch fabric modules.
- Use the **show linecard** command to display information for the line cards.

To make the slot configuration persistent across a chassis reboot (which involves reloading the management modules), you must save the configuration persistently by issuing the **copy running-config startup-config** command after the line card reaches the online state and before the system reboots.

## Replacing a line card

You can remove a line card without powering it off. However, doing so will not remove the configuration. When you replace a card with a different type, you must first remove the configuration and then reconfigure the slot for the new line card type.

Install a new line card only if it is supported by the firmware running in the chassis. Inserting a line card into a chassis running firmware that does not support the line card may result in unexpected behavior.

Complete the following steps to replace a line card.



### CAUTION

Removing the configuration requires the card to be powered off.

1. Power off the line card by issuing the **power-off linecard** command followed by the slot number.
2. Enter the **configure terminal** command to enter global configuration mode.
3. Enter the **rbridge-id rbridge-id** command to enter RBridge ID configuration mode.
4. Enter the **no linecard slot\_number** command to clear the slot configuration.
5. Remove the line card.
6. Enter the **linecard slot\_number** command followed by a question mark (?) to display the line card menu.
7. Select a line card type and enter the **linecard slot\_number linecard\_type** command.
8. Enter the **exit** command twice to return to privileged EXEC mode.
9. Insert the new line card into the configured slot.
10. Enter the **power-on linecard** command to power on the line card.
11. Save the configuration persistently by issuing the **copy running-config startup-config** command after the line card reaches the online state.
12. Verify the configuration with the **show running-config linecard linecard** command.

```

switch# power-off linecard 4
switch# configure terminal
Entering configuration mode terminal
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)# no linecard 4

```

```

switch(config-rbridge-id-1)# linecard 4 ?
Possible completions:
LC12x40G  12X40G linecard
LC48x1G   48X1G linecard
LC48x10G 48X10G linecard
LC72x1G  72X1G linecard
LC48x10GT 48X10G Base-T linecard
LC27X40G  27X40G linecard
LC6X100G  6X100G linecard
switch(config-rbridge-id-1)# linecard 4 LC48x10G
Creating new linecard configuration was successful.
switch(config-rbridge-id-1)# exit
switch(config)# exit
switch# copy running-config startup-config
switch# show running-config rbridge-id 4 linecard
rbridge-id 1
linecard 1 LC48x10G
linecard 4 LC48x10G

```

## Configuring High Availability

The following sections provide you with information on configuring High Availability (HA) support on Brocade switches.

### Using HA commands

A variety of High Availability (HA) commands are available on the switch in privileged EXEC mode.

- **show ha** displays the management module status.

```

switch# show ha
Local (M2): Active, Cold Recovered
Remote (M1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized

```

- **ha failover** forces the active management module to fail over. The standby management module will take over as the active management module. This command is only available in a modular chassis system.
- **reload system** reboots the entire chassis. This command is supported only on the active management module. This command is not supported on the standby management module. Both management modules must be in sync for the HA reboot operation to succeed. In logical chassis cluster mode, this command can be issued from the principal node to reset one remote node or all of the remote nodes by specifying either the individual *rbridge-id* or **all**.
- **ha sync start** enables HA state synchronization after an **ha sync stop** command has been invoked.
- **show ha all-partitions** displays details for all line cards and the MM HA state.

#### NOTE

For additional HA commands and related commands, refer to the *Network OS Command Reference*.

### Understanding expected behaviors for reload and failover

The following tables identify expected behaviors that result from controlled and uncontrolled reload and failover conditions.

#### NOTE

When MMs are out of sync, the **reload** command does not work. Use the **reload system** command to reboot the switch in this case.

TABLE 14 Expected behaviors for controlled reload and failover

Command syntax	Behavior in fabric cluster and logical chassis cluster	Behavior in compact switches
<b>reload</b>	Cold failover to standby management module (MM).	Reloads the switch
<b>reload standby</b>	Reboot the standby MM.	Not available
<b>reload system</b>	Reboot both MMs. MMs will retain the HA roles.	Reloads the switch
<b>ha failover</b>	Causes a reset on the active MM and a warm recovery on the standby MM. All existing telnet sessions are required to be restarted.	Not available

TABLE 15 Expected behaviors for uncontrolled failover

Command syntax	Behavior in fabric cluster and logical chassis cluster	Behavior in compact switches
Panic	Warm failover to standby MM.	Reloads the switch
MM removal	Warm failover to standby MM.	Not available
Power cycle	MMs will retain the HA roles upon booting up.	Resets the switch

## Disabling and enabling a chassis

The chassis is enabled after power is turned on, and diagnostics and switch initialization routines have finished. All interfaces are online. You can disable and re-enable the chassis as necessary.

- Use the **chassis disable** command if you want to take all interfaces offline. If the switch was part of an Ethernet fabric, the fabric reconfigures.
- Use the **chassis enable** command to bring the interfaces back online. All interfaces that were enabled before the chassis was disabled are expected to come back online. If the switch was part of an Ethernet fabric, it rejoins the fabric.

### NOTE

Disabling the chassis is a disruptive operation. Use the **shutdown** command to disable or enable a few selected interfaces only. Refer to the *Network OS Command Reference* for more information on this command.

## Rebooting a switch

Network OS provides several commands to reboot your system: **reload**, **fastboot**, and **reload system**.



### CAUTION

All reboot operations are disruptive, and the commands prompt for confirmation before executing. When you reboot a switch connected to a fabric, all traffic to and from that switch stops. All ports on that switch remain inactive until the switch comes back online.

## Rebooting a Top-of-Rack switch

- The **reload** command performs a "cold reboot" (power off and restart) of the control processor (CP). If the power-on self-test (POST) is enabled, POST is executed when the system comes back up.
- The **fastboot** command performs a "cold reboot" (power off and restart) of the control processor (CP), bypassing POST when the system comes back up. Bypassing POST can reduce boot time significantly.



**CAUTION**

Do not perform a reload command between a chassis disable command and a chassis enable command. Your ports will be closed.

## Rebooting a modular chassis

A chassis reboot brings up the system in sequential phases. First, software services are launched on the management modules and brought up to the active state. Then, the line cards are powered on and initialized. Software services are launched on the line cards and brought up to the active state. When the line card initialization reaches the final state, the chassis is ready to accept user commands from the CLI interface.

During the boot process system initialization, configuration data (default or user-defined) are applied to the switch through configuration replay. For more information, refer to [Managing configurations across redundant management modules](#) on page 120.

- On a modular chassis, the **reboot** and the **fastboot** commands only reboot the management module on which the command is executed. If you log in to the switch IP address and execute one of these commands, only the active management module reboots and POST is bypassed.
- The **reload system** command performs a "cold reboot" (power off and restart) of the entire chassis. If the power-on self-test (POST) is enabled, POST is executed when the system comes back up.

## Troubleshooting switches

This section presents an overview of a variety of techniques for capturing data and system messages, which can be helpful in interactions with technical support.

### Capturing and managing supportSave data

If you are troubleshooting a production system, you will have to capture data for further analysis or send the data to your switch service provider. The **copy support** command provides a mechanism for capturing critical system data and uploading the data to an external host or saving the data to an attached USB device.

### Uploading supportSave data to an external host

To upload supportSave data interactively, enter the **copy support-interactive** command and provide input as prompted. Specifying an IPv6 address for the server requires Network OS v3.0.0 or later. For a non-interactive version of the command, refer to the *Network OS Command Reference*.

```
switch# copy support-interactive

Server Name or IP Address: 10.38.33.131
Protocol (ftp, scp): ftp
User: admin
Password: *****
Directory: /home/admin/support
VCS support [y/n]? (y): n
Module timeout multiplier [Range: 1 to 5. Default: 1]: 1

copy support start
Saving support information for chassis:sw0, module:RAS...(output truncated)
```

### Saving supportSave data to an attached USB device

You can use a Brocade-branded USB device to save the support data. The Brocade-branded USB device comes with factory-configured default directories and interacts with the Network OS CLI.

1. Enter the **usb on** command to enable the USB device.



### Displaying the autoupload configuration

Enter the **show running-config support autoupload-param** command to display the autoupload configuration on the local switch.

```
switch(config)# do show running-config support autoupload-param

support autoupload-param hostip 10.31.2.27 username supportadmin directory /users/support/ffdc_autoupload
protocol ftp password "3iTYxJWEUHp9axZQt2tbvw==\n"
```

### Using additional supportSave commands

Use the following commands to configure additional supportSave data collection parameters:

- Use the **show support** command to display a list of core files on the switch.
- Use the **clear support** command to erase support data on the switch.

Refer to the *Network OS Command Reference* for more information on these commands.

### Logging error messages

Network OS provides several mechanisms for logging error messages including syslog, RASLog, and audit log. The types of message logging available and the setup procedures are documented in the "Introduction to Brocade Error Message Logging" chapter of the *Network OS Message Reference Manual*.

## Configuring policy-based resource management and hardware profiles

The policy-based resource management feature allows users to make better use of hardware resources. In particular, pre-made profiles are provided that optimize ASIC resources for Keep-Alive Protocol (KAP) profiles, route-table profiles, and ternary content-addressable memory (TCAM) profiles. The profiles are enabled by keywords available under the **hardware-profile** command in RBridge ID configuration mode. The switched-based hardware profile configuration is local to an RBridge within a VCS Fabric.

#### ATTENTION

This is a disruptive command. In order for the last update of the hardware profile configuration to take effect on a switch, the switch has to be rebooted. In logical chassis cluster mode, use the **reload system** command. In fabric cluster mode, execute the **copy running-config startup-config** command, followed by the **reload system** command.

## Configuring KAP profiles

### KAP profile overview

The Keep-Alive Protocol (KAP) profile feature allows users to allocate hardware resources to various keep-alive protocols. As a result, during a failover, those protocols can continue to send keep-alive packets to network neighbors and maintain connectivity, achieving a hitless failover. Users now have the flexibility of defining custom KAP profiles for the following protocols: LACP, XSTP, RPVST, UDLD, BFD-VXLAN, BFD-L3, and FCoE. In addition, default KAP profiles are predefined for the supported platforms.

There are two types of entries for the resources allocated to KAP applications: hardware and software. With hardware entries, the switch continues to send keep-alive packets even during an HA failover; with software entries, the keep-alive packets are resent only after the failover process is completed.

## Default KAP profile

By default, the switch comes up with a default KAP profile. With this profile, any protocol that requests a KAP entry gets it first, with requests processed on a first-come, first-served basis. The switch processes the hardware entries first. When those are consumed, the switch begins allocating new KAP entries from the software entry pool.

## Custom KAP profiles

A custom KAP profile is defined globally within a cluster and applied to individual switches. Normally, a user would define a global KAP profile for each type of switch, based on physical capability and deployment requirements. The user can define as many custom KAP profiles as needed, each with a unique name and parameter settings.

The **custom-profile** option is applied in hardware configuration mode, by means of the global **hardware** command. Then, by means of the **kap** keyword, the user can create custom named instance and select from among the available protocols. Profiles include the keep-alive interval and the number of keep-alive entries per slot. The following example illustrates this process, with the **show running-config hardware custom-profile** command used to verify the configuration.

```
device(config)# hardware
device(config-hardware)# ?
Possible completions:
connector          Configure a connector
connector-group    Configure a connector group
custom-profile     Configure customized hardware profiles
describe          Display transparent command information
do                Run an operational-mode command
exit              Exit from current mode
flexport          Option to change the Ethernet port to FibreChannel port
help              Provide help information
no                Negate a command or set its defaults
port-group        Configure a port-group
pwd               Display current mode path
top               Exit to top level and optionally run command
device(config-hardware)# custom-profile kap myprofile
device(config-kap-myprofile)# ?
Possible completions:
bfd-l3             Configure BFD-L3 protocol KAP parameters
bfd-vxlan          Configure BFD-VXLAN protocol KAP parameters
describe          Display transparent command information
do                Run an operational-mode command
exit              Exit from current mode
fcoe              Configure FCOE protocol KAP parameters
help              Provide help information
lACP              Configure LACP protocol KAP parameters
no                Negate a command or set its defaults
pwd               Display current mode path
rPvSt             Configure rPvSt protocol KAP parameters
top               Exit to top level and optionally run command
uDLd              Configure uDLd protocol KAP parameters
xSTP              Configure xSTP protocol KAP parameters
device(config-kap-myprofile)#
device(config-kap-myprofile)# udlld num-entry 64
device(config-kap-myprofile)# lacp hello-interval 30000 num-entry 50
device(config-kap-myprofile)# bfd-vxlan hello-interval 300 num-entry 20
device(config-kap-myprofile)# xstp num-entry 64
device(config-kap-myprofile)# bfd-l3 num-entry 100
device(config-kap-myprofile)# fcoe num-entry 64
device(config-kap-myprofile)# rpvst num-entry 128
device# show running-config hardware custom-profile
hardware
  custom-profile kap myprofile
    lacp hello-interval 30000 num-entry 50
    xstp num-entry 64
    rpvst num-entry 128
    udlld num-entry 64
    bfd-vxlan hello-interval 300 num-entry 20
    bfd-l3 num-entry 100
    fcoe num-entry 64
```

**NOTE**

The "hello-interval" and "num-entry" parameters are optional. If they are not specified, default values are used.

The profile "myprofile" can now be applied to multiple switches in the cluster. The settings are dependent on the platform and the user application. For a custom profile to take effect, it has to be applied to a switch in RBridge ID configuration mode, as illustrated in the following section. When a global custom profile is defined, only a generic validation process is performed, not a platform-specific validation.

Once a custom KAP profile is activated on one or more switches, the profile cannot be modified or deleted. To change custom profile settings on a switch, the user must first define a new custom KAP profile and apply it to the switch. Only when a custom profile is no longer applied to any switch in the cluster can that profile be modified or deleted, as shown below.

```
device(config-hardware)# no custom-profile kap myprofile
```

**NOTE**

All of the protocol types listed in the menu above support the **no** keyword. This allows the user to delete all or part of the settings for the protocol. If a custom setting for a protocol is removed from a custom KAP profile, the default KAP setting for that protocol is applied.

## Switch-based KAP profile

This following example illustrates how to apply a custom KAP profile to a specific switch. This is done in RBridge ID configuration mode, by means of the **hardware-profile** command with the **kap** keyword. The configuration is verified by means of the **show running config rbridge-id** command with the **hardware-profile** keyword.

```
device(config-rbridge-id-85)# hardware-profile ?
Possible completions:
  kap                Select KAP profile type
  route-table       Select route table profile type
  tcam              Select TCAM profile type
device(config-rbridge-id-85)# hardware-profile kap ?
Possible completions:
  custom-profile    Customized profile
  default          Basic support for all applications
device(config-rbridge-id-85)# hardware-profile kap custom-profile myprofile
%Warning: To activate the new profile config, please run 'reload system' on the target switch.

device# show running-config rbridge-id 85 hardware-profile
rbridge-id 85
hardware-profile tcam default
hardware-profile route-table ipv4-max-arp maximum_paths 32
hardware-profile kap custom-profile myprofile
```

When a custom KAP profile is applied, a validation process checks whether the specified custom profile exists. Then a platform-dependent validation of the custom profile is triggered. Both the parameter settings for individual protocols and the total entries are checked against platform capabilities. As with other hardware profiles, the switch must be rebooted for changes to take effect.

## Limitations

The KAP profile feature is supported for both fabric cluster and logical chassis cluster modes in Network OS 6.0.1 and later. However, note the following limitations for each mode.

### Limitations in logical chassis cluster mode:

If the user executes the **copy default-config startup-config** command on a switch in logical chassis cluster mode, the KAP profile settings in the hardware are set to the default following a reboot. This occurs even if there is a mapping of a KAP profile setting to a

custom KAP profile that has been removed as a result of the global configuration reverting to the default state. Other hardware profile settings are maintained.

In this case, if the switch is a rejoining secondary node, then the mismatch between the local setting and the configuration saved in the cluster will trigger a RASLOG message that notifies the user to reboot the switch in order to resolve the inconsistency.

#### Limitations in fabric cluster mode:

If the user sets a switch to boot up from a startup-config file instead of startup-DB, and the startup-config file contains a KAP profile setting that is mapped to a custom profile, then the KAP profile is set to the default in the running-config file and in the database after the switch boots up.

This case can occur when the user executes the **copy file startup-config** command and reboots, and the file has a KAP profile setting that maps to a custom KAP profile. In this case, the user must reconfigure the KAP profile manually to the desired custom profile after the switch is initially up, and then reboot the switch again.

## Configuring route-table profiles

Route-table profiles can be optimize in hardware.

The following table describes the available command options (keywords) to optimize route profiles, available under the **route-table** keyword in turn under the **hardware-profile** command (refer to the *Network OS Command Reference*).

**TABLE 16** Options for optimizing route-table profiles

Keyword	Optimizes resources for . . .
<b>default</b>	Basic IPv4/IPv6 dual-stack operations
<b>ipv4-max-arp</b>	Maximum number of IPv4 ARP entries
<b>ipv4-max-route</b>	Maximum number of IPv4 routes
<b>ipv4-min-v6</b>	IPv4 routes in dual-stack configurations
<b>ipv6-max-nd</b>	Maximum number of IPv6 Neighbor Discovery entries
<b>ipv6-max-route</b>	Maximum number of IPv6 routes
<b>kap</b>	Keep-alive profiles
<b>maximum_paths</b>	Maximum number of ECMP paths (8, 16, 32)
<b>openflow</b>	OpenFlow support
<b>route-table</b>	Route profiles

With the Network OS 6.0.1, two new keywords were added, available under the route-table profile type.

- The **maximum-paths** keyword allows the user to configure the maximum number of ECMP paths. This keyword is optional. If not selected, the maximum-path configuration remains unchanged. The valid values are 8, 16, and 32, with 8 the initial default. (Once the latter value is changed, it must be reentered explicitly, which is different from previous releases.) As with other changes to the hardware profile, the switch must be rebooted for changes to take effect.
- The **openflow** keyword allows the user to enable or disable support for the OpenFlow feature in the route-table profile. This keyword is optional. If it is not used, the OpenFlow profile setting is unchanged. This keyword is also available under the TCAM profile. (Refer to the following section.)

The following example specifies maximum paths and disables OpenFlow in the TCAM profile, and then confirms the configuration.

```
device(config-rbridge-id-67)# hardware-profile route-table ipv4-max-arp ?
Possible completions:
  maximum_paths  Maximum number of load-sharing paths
  openflow       Enable/disable openflow support
  <cr>
device(config-rbridge-id-67)# hardware-profile route-table ipv4-max-arp maximum-path 16
%Warning: To activate the new profile config, please run 'reload system' on the target switch.

device# show running-config rbridge-id hardware-profile
rbridge-id 67
  hardware-profile tcam default
  hardware-profile route-table ipv4-max-arp maximum-path 16 openflow off
  hardware-profile kap default
```

The following example selects a route-table profile to optimize resources for the maximum number of IPv6 Neighbor Discovery entries:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# hardware-profile route-table ipv6-max-nd
%Warning: To activate the new profile config, please run 'reload system' on the target switch.
```

#### NOTE

When you use the **hardware-profile route-table ?** command to see the available options, the currently applied hardware profile is at the top of the list and is enclosed by square brackets ([ ]).

## Configuring TCAM profiles

TCAM profiles can be optimized in hardware.

The following table describes the available command options (keywords) to optimize TCAM profiles, available under the **tcam** keyword.

**TABLE 17** Options for optimizing TCAM profiles

Keyword	Optimizes resources for . . .
<b>default</b>	Basic support for all applications
<b>dyn-arp-insp</b>	Dynamic ARP inspection (DAI)
<b>ipv4-v6-mcast</b>	Multicast
<b>ipv4-v6-pbr</b>	IPv4 and IPv6 ACLs and policy-based routing tables
<b>ipv4-v6-qos</b>	IPv4 and IPv6 ACLs and QoS
<b>l2-ipv4-acl</b>	Layer 2 and IPv4 ACLs
<b>l2-acl-qos</b>	Layer 2 ACLs and QoS
<b>openflow</b>	OpenFlow support

With Network OS 6.0.1, two new keywords were added.

- The **dyn-arp-insp** keyword allows the user to configure optimized dynamic ARP inspection (DAI).
- The **openflow** keyword allows the user to enable or disable support for the OpenFlow feature in the TCAM profile.

The OpenFlow feature requires consistency between the route-table and TCAM profile configurations. This consistency is enforced automatically. When the user selects **openflow** for a TCAM profile, the route-table profile is set to OpenFlow support, which is enabled on top of the current setting. Similarly, when the user selects any other type of TCAM profile that does not support OpenFlow, the route-table profile is automatically set to disable OpenFlow support. If the user first disables OpenFlow support in the route-table profile, then the TCAM profile is set to the default subtype. To specify a nondefault TCAM subtype, the user must specify that choice in the TCAM

menu. If the user first specifies OpenFlow support in the route-table profile, then the TCAM profile is set automatically to support OpenFlow. Status messages report consistency between the two types of profiles, as in the following configuration examples.

```
device(config-rbridge-id-2)# hardware-profile tcam ?
Possible completions:
 [openflow]
 default          basic support for all applications
 dyn-arp-insp     optimized for dynamic Arp Inspection
 ipv4-v6-mcast    optimized for multicast
 ipv4-v6-pbr      optimized for IPv4 and IPv6 ACL, PBR
 ipv4-v6-qos      optimized for IPv4 and IPv6 ACL, QOS
 l2-acl-qos       optimized for L2 ACL, QOS
 l2-ipv4-acl      optimized for L2 and IPv4 ACL
 openflow         optimized for openflow support
device(config-rbridge-id-2)# hardware-profile tcam openflow
%INFO: Openflow is also enabled in route-table profile.
%Warning: To activate the new profile config, please run 'reload system' on the target switch.
```

```
device# show running-config rbridge-id hardware-profile
rbridge-id 2
 hardware-profile tcam openflow
 hardware-profile route-table ipv4-max-arp maximum_paths 8 openflow on
 hardware-profile vlan-classification default
 hardware-profile kap default
```

```
device(config-rbridge-id-2)# hardware-profile tcam default
%INFO: Openflow is also disabled in route-table profile.
%Warning: To activate the new profile config, please run 'reload system' on the target switch
sw0# show running-config rbridge-id hardware-profile
rbridge-id 2
 hardware-profile tcam default
 hardware-profile route-table ipv4-max-arp maximum_paths 8 openflow off
 hardware-profile vlan-classification default
 hardware-profile kap default
```

```
device(config-rbridge-id-2)# hardware-profile route-table ipv4-max-arp ?
Possible completions:
 maximum_paths  Maximum number of load-sharing paths
 openflow       Enable/disable openflow support
 <cr>
```

```
device(config-rbridge-id-2)# hardware-profile route-table ipv4-max-arp openflow ?
Possible completions:
 [on]
 off  Disable openflow
 on   Enable openflow
device(config-rbridge-id-2)# hardware-profile route-table ipv4-max-arp openflow on
%INFO: The TCAM profile has been set to openflow.
%Warning: To activate the new profile config, please run 'reload system' on the target switch
```

```
device# show running-config rbridge-id hardware-profile
rbridge-id 2
 hardware-profile tcam openflow
 hardware-profile route-table ipv4-max-arp maximum_paths 8 openflow on
 hardware-profile vlan-classification default
 hardware-profile kap default
```

```
device(config-rbridge-id-2)# hardware-profile route-table ipv4-max-arp openflow off
%INFO: The TCAM profile has been set to default. For more granular TCAM selections, please use the TCAM
menu.
%Warning: To activate the new profile config, please run 'reload system' on the target switch.
```

```
device# show running-config rbridge-id hardware-profile
rbridge-id 2
 hardware-profile tcam default
 hardware-profile route-table ipv4-max-arp maximum_paths 8 openflow off
 hardware-profile vlan-classification default
 hardware-profile kap default
```



The following example illustrates the configuration of optimization for DAI.

```
switch(config-rbridge-id-2)# hardware-profile ?
Possible completions:
  kap                Select KAP profile type
  route-table       Select route table profile type
  tcam              Select TCAM profile type
device(config-rbridge-id-2)# hardware-profile tcam ?
Possible completions:
  [openflow]
  default           basic support for all applications
  dyn-arp-insp     optimized for dynamic Arp Inspection
  ipv4-v6-mcast    optimized for multicast
  ipv4-v6-pbr      optimized for IPv4 and IPv6 ACL, PBR
  ipv4-v6-qos      optimized for IPv4 and IPv6 ACL, QOS
  l2-acl-qos       optimized for L2 ACL, QOS
  l2-ipv4-acl      optimized for L2 and IPv4 ACL
  openflow         optimized for openflow support
device(config-rbridge-id-2)# hardware-profile tcam dyn-arp-insp
%Warning: To activate the new profile config, please run 'reload system' on the target switch
```

Note the following additional conditions for TCAM profiles:

- TCAM profiles affect only ACLs, policy-based routing (PBR), flow-based QoS, and multicast entries, without affecting other features, protocols, or hardware resources.
- The TCAM profile options (listed in the table) are not customizable or configurable, and they may not be appropriate to all network designs.
- The following QoS features are optimized by TCAM profiles:
  - Flow-based QoS and flow-based policing for Layer2/Layer 3 ingress and egress
  - System Qos (VLAN-based) for Layer2/Layer 3 ingress and egress
  - Auto NAS
  - Storm control
  - Flow-based SPAN and RSPAN, including VXLAN based
  - Flow-based Sflow, including VXLAN based
- The following QoS features are not affected by TCAM profiles:
  - All port-based QoS features (RED; PFC and legacy flow control; CoS mutation, DSCP CoS, DSCP traffic class, DSCP mutation; scheduling, shaping, and port-based policing)
  - Port-based SPAN and RSPAN
  - Port-based Sflow

## Guidelines for changing hardware profiles

Note the following guidelines for changing hardware profiles:

- In fabric cluster and logical chassis cluster mode, you must reload the target switch after changing a switch-based profile for the new profile to take effect.
  - In logical chassis mode, when a secondary switch rejoins the cluster with a default profile configuration while the profile configuration for the secondary switch is "nondefault" on the principle switch, you must reload the secondary switch again after it has rejoined the cluster for the nondefault profile to take effect. The TCAM and route-table hardware profiles are persistent across a "copy default-config startup-config" operation.
  - In fabric cluster mode, you must use the **copy running-config startup-config** command first, before reloading the switch.
- After a Netinstall or a firmware upgrade, the default profiles are automatically set for all hardware types, with OpenFlow disabled and maximum-paths set to 8. Also, the profile configuration defaults after changing a switch VCS ID or RBridge ID. However, the current profile persists after the **copy default-config startup-config** command completes and the switch reboots. Additionally, the current profile persists after a VCS mode change.

- There is no "no" option for the switch-based hardware-profile command, because switch-based hardware profiles always exist, with either the default or one of the nondefault configurations.
- When you change a hardware profile, the supported scale numbers remain the same with respect to the configuration even if hardware may not be able to fulfill them. This ensures that the same protocol and interface information remain valid with all hardware profile settings.

## Using hardware profile show commands

The following **show** commands can be used to verify the status of hardware profiles. For details, refer to the *Network OS Command Reference*.

**TABLE 18** Network OS show commands

Command	Description
<b>show hardware-profile</b>	Displays the current active profile information and subtype details for each profile type and RBridge ID on local switch or specified RBridge ID or all switches in LC cluster. For complete details on the <b>show hardware-profile</b> command, refer to the <i>Network OS Command Reference</i> .
<b>show running-config rbridge-id hardware-profile</b>	Displays the enabled route table and TCAM profiles in the running configuration for all RBridge IDs, or a specific enabled RBridge ID.
<b>show running-config hardware custom-profile</b>	Displays user-defined custom profiles. (With the initial release, only custom KAP profiles are supported.)

The **show hardware-profile** command supports logical chassis cluster-wide hardware profile information. To view the current hardware-profile information on other switches in the cluster, specify an RBridge ID as in the following example.

```
device# show hardware-profile rbridge-id 89 current
```

This also applies to the predefined hardware-profile information of the selected type. The predefined hardware-allocation details for the target platform are retrieved and displayed as for the following example command.

```
device# show hardware-profile rbridge-id 91 tcam ipv4-v6-qos
```

To display hardware profile information for all switches in the cluster at one time, use the **rbridge-id all** keywords as in the following examples:

```
device# show hardware-profile current rbridge-id all
```

```
device# show hardware-profile rbridge-id all route-table ipv6-max-nd openflow
```

## Hardware-profile upgrade/downgrade considerations

During an upgrade from Network OS 5.x or 6.0.0 to Network OS 6.0.1, the database conversion and startup-file replay of hardware profile configurations is fully supported. After the upgrade, the hardware profile settings are as follows:

- TCAM settings are unchanged.
- Route-table settings are unchanged.
- KAP settings are set to the default.
- ECMP maximum-path settings are set to 8.
- OpenFlow settings are set to disabled.

During a downgrade from Network OS 6.0.1 to 6.0.0 or 5.x, the user must first do the following to be allowed to proceed with the downgrade:

- Set the KAP profile to the default.
- Disable OpenFlow.
- Set ECMP maximum-paths to 8.
- Disable TCAM DIA and OpenFlow optimization.

#### NOTE

Because of the extension of the route-table profile parameters, during a downgrade the replaying of the ASCII configuration file collected from Network OS 6.0.1 to any prior releases is not supported for the **hardware-profile route-table** command.

## Auto Fabric

Auto Fabric is a feature that allows plug-and-play for Brocade VDX switches.

A type of configuration known as *bare-metal* is required for a switch to join an existing VCS cluster by means of plug and play. The cluster must be a logical chassis cluster.

Bare-metal configuration is a profile that contains a WWN-to-RBridge ID mapping. You first must pre-configure this mapping in the existing VCS cluster to allow the bare-metal switch to join the cluster. A switch with its bare-metal flag set to true (which is the factory default) can request the following required configuration settings from a physically connected neighbor that already belongs to the cluster:

- VCS ID
- RBridge ID
- VCS mode
- Global VLAN state

From this information, the bare-metal switch auto-configures itself and reboots with the bare-metal flag now disabled. (Any configuration performed on the switch disables the bare-metal flag, but you may need to toggle the ISL. However the bare-metal configuration on the remaining nodes in the cluster remains intact. ) Bare-metal state must be disabled for cluster formation to occur.

#### NOTE

If VCS parameters are not set, the switch returns to the bare-metal-enabled state if you issue a **write erase** command, or if you do a Netinstall. In addition, if VCS parameters are not set, the **firmwaredownload default-config** command also returns the switch to the bare-metal-enabled state.

## Configuring Auto Fabric for bare metal

Bare-metal configuration requires a unique WWN-to-RBridge ID mapping, which informs the cluster which RBridge ID can be assigned to a joining bare-metal switch. Each time you want to add a bare-metal switch to a cluster, you need to create a new WWN-RBridge-ID mapping that is unique for the cluster.

The cluster must be a logical chassis cluster, and this configuration must be executed the principal node in that cluster. Run the **show vcs** command on the bare-metal switch to obtain its WWN.

To create a bare-metal configuration, do the following:

1. Enter the **configuration** command to enter global configuration mode:

```
switch# configure
```

2. Enter the **preprovision** command to map an RBridge ID to the WWN name of the bare-metal switch you will be adding to the cluster. This can be any RBridge ID that is not currently assigned within the cluster. For example, if the WWN of the bare-metal switch is 10:11:12:13:14:15:16:17, and you wish to assign an RBridge of 5 to the bare-metal switch, you would enter:

```
switch (config)# preprovision rbridge-id 5 wwn 10:11:12:13:14:15:16:17
```

#### NOTE

If you want to change this Rbridge-ID assignment after you have issued the above command, refer to the [Changing RBridge-ID-to-WWN mapping for bare-metal configuration](#) on page 100.

3. Physically connect the bare-metal switch to the cluster.

The bare-metal switch obtains its VCS ID, VCS mode, Virtual-Fabric state, and RBridge ID from its neighbor, then the bare-metal switch automatically reboots. After reboot is completed, the switch is now bare-metal disabled. The cluster then verifies that the RBridge ID of the bare-metal switch is unique to the cluster and to the RBridge-ID-to\_WWN mapping, then adds the switch to the cluster.

#### NOTE

if a node is part of cluster but is in offline state, and the node was baremetal-enabled, then the node obtains its RBridge-ID, VCS ID, and configuration from the cluster.

Each time you want to add a bare-metal switch, you need to repeat this procedure with the WWN name of the bare-metal switch by mapping it to an RBridge ID that is not currently assigned within the cluster.

## Changing RBridge-ID-to-WWN mapping for bare-metal configuration

If you have configured the RBridge-ID-to-WWN mapping for a bare-metal switch, but have not yet plugged the switch into the cluster, you can still change the RBridge ID that will be assigned to the bare-metal switch.

Do the following on the principal switch to change the mapping:

1. Use the **no preprovision** command to remove a currently configured mapping. For example, if you already ran the command **preprovision rbridge-id 5 wwn 10:11:12:13:14:15:16:17**, and you want to remove this configuration, enter the following command:

```
switch (config)# no preprovision rbridge-id 5 wwn 10:11:12:13:14:15:16:17
```

#### NOTE

To display the currently configured RBridge-ID-to-WWN mapping, enter the **show running-config preprovision** command. To update only the WWN and not the RBridge ID, use the **preprovision** command with the RBridge ID whose WWN mapping you wish to change. For example, if you have already configured RBridge ID 5 to map to a WWN of 10:11:12:13:14:15:16:17, and you want to change the WWN to 11:11:11:11:11:11:11, you would enter the following command: **preprovision rbridge-id 5 wwn 11:11:11:11:11:11:11** command.

2. Enter the **preprovision** command containing the new RBridge ID-to-WWN mapping. For example, if you now want RBridge ID 6 to be assigned to the bare-metal switch referenced in the previous step, enter the following command:

```
switch (config)# preprovision rbridge-id 6 wwn 10:11:12:13:14:15:16:17
```

#### NOTE

To delete all configured RBridge-ID-to-WWN mappings, enter the **no preprovision rbridge-id** command. This removes all mappings under the previous container, so that the **show running-config preprovision** command will return "% No entries found."

## Using maintenance mode for graceful traffic diversion (VCS Fabrics only)

Maintenance mode diverts all possible traffic through a switch under maintenance to other switches in the cluster, while leaving the switch under maintenance as part of the cluster.

The following sections provide an overview and configuration examples, respectively.

### Overview of maintenance mode

Prior to Network OS 7.0.0, during maintenance activity the user had to shut down all interfaces one by one to minimize traffic disruption, resulting in the switch leaving the VCS Fabric.

During a firmware upgrade or debugging activity, the user had to disable all edge and ISL ports. This caused data traffic to be lost and the node to leave the cluster, becoming inaccessible from the principle node. Maintenance mode keeps the ISL ports enabled, and existing traffic is gracefully diverted to other nodes in the cluster. The edge ports become administratively down, and the path cost of the node's ISL ports are set to such a high value that traffic through a node in maintenance mode is not preferred when an alternate path is available. The node remains part of the fabric, minimizing traffic disruption in case of an unexpected reload during maintenance.

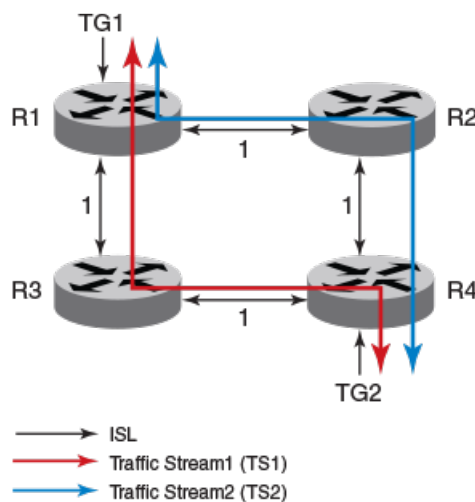
In the case of vLAGs, if a vLAG member port is shut down abruptly, there can be a black-holing of traffic that lasts a few second. When maintenance mode is enabled, other vLAG member nodes in the cluster are notified to take over the traffic, avoiding loss of traffic.

The following figures illustrate the flow of two traffic streams (TSs) from two traffic generators (TGs) before and after maintenance mode is applied.

#### NOTE

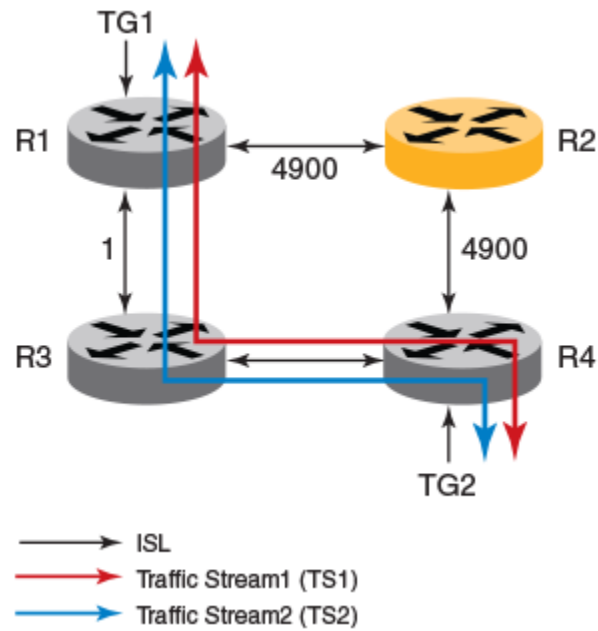
Traffic is diverted only if an alternative path is available. The user is responsible for ensuring that traffic has a path other than through the node under maintenance.

FIGURE 15 Traffic flow: All R Bridges online (before maintenance mode)



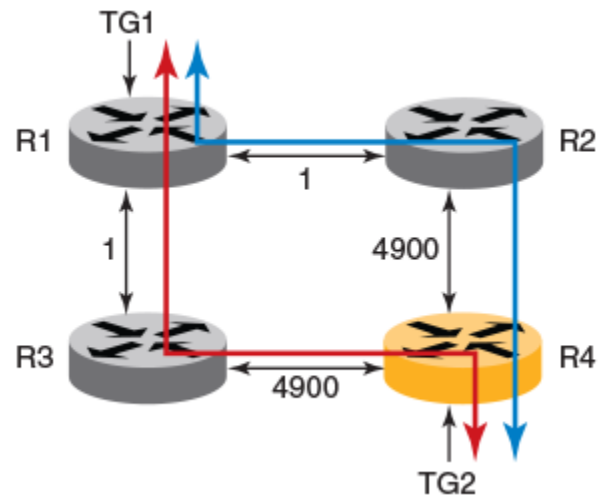
- All nodes in VCS Fabric are in online state
- Path cost of all ISLs is 1
- TS1 flow: TG1 > R1 > R3 > R4 > TG2
- TS2 flow: TG1 > R1 > R2 > R4 > TG2

FIGURE 16 Traffic flow: Intermediate RBridges in maintenance mode



- R2 set to maintenance mode
- Path cost of all ISLs connecting to R2 increased to 4900 (infinity)
- Traffic takes available low-cost alternate paths
- TS1 flow: TG1 > R1 > R3 > R4 > TG2
- TS2 flow: TG1 > R1 > R3 > R4 > TG2

FIGURE 17 Traffic flow: No alternate path available



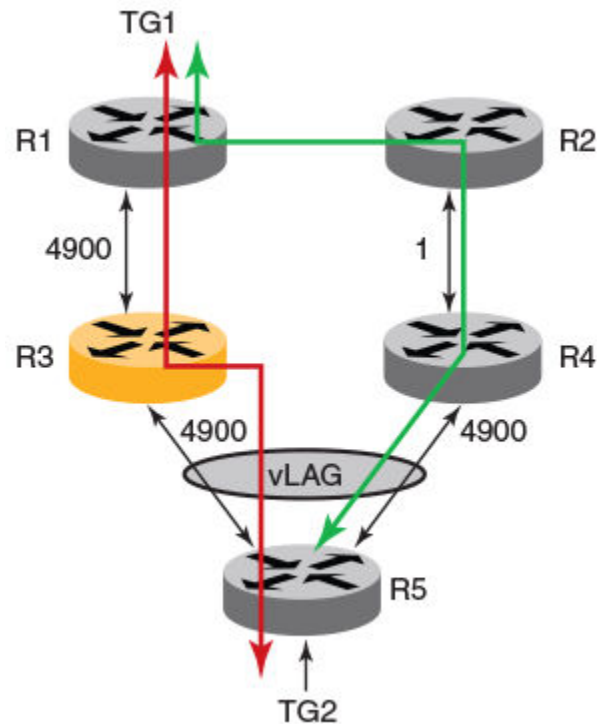
- R4 set to maintenance mode
- Path cost of all ISLs connecting to R4 increased to 4900 (infinity)
- No alternate path for TS1 and TS2 (traffic takes same path)

**NOTE**

Because R4 is in maintenance mode, the TG2 edge interface is in the administratively down state, resulting in traffic disruption. The user must enable the TG2 edge interface manually for traffic to resume while R4 is in maintenance mode.

- TS1 flow: TG1 > R1 > R3 > R4 > TG2
- TS2 flow: TG1 > R1 > R2 > R4 > TG2

FIGURE 18 Traffic flow: vLAG member



- Initially R3 carries vLAG traffic between TG1 and TG2
- TS1 flow: TG1 > R1 > R3 > R5 > TG2
- R3 set to maintenance mode, notifies R4 to take over vLAG traffic. The R3 link is shut down because the vLAG link is considered to be an edge port.
- TS2 flow: TG1 > R1 > R2 > R4 > R5 > TG2

### Additional considerations and limitations for maintenance mode

Note the following:

- The maintenance mode feature is supported in both logical chassis cluster and fabric cluster modes.
- The maintenance mode configuration and the administrative state of the ports persists across reboots and ISSU/firmware updates.
- It is possible to change the administrative state of any interface while in maintenance mode, but enabling or modifying port-channel and port-channel member ports are not supported.
- If a port-channel or port-channel member configuration is modified while in maintenance-mode, the user should remove and reconfigure the port-channel and port-channel member after exiting maintenance mode.
- ISL ports that are shut down while in maintenance mode will be preserved after maintenance mode is disabled.
- When maintenance mode is disabled, the original user-configured administrative state of the edge ports is restored.
- ISSU and HA failover are supported during maintenance mode.
- Maintenance mode is not persistent in the case of copying the default-config to the startup-config, or a mode change from fabric cluster mode to logical chassis cluster mode.
- Maintenance mode does not restrict any file-copy operations.



- If the switch is the root of a multicast tree, it remains part of a TRILL multicast tree.

## Maintenance mode behavior under various scenarios

The following table summarizes the behavior of maintenance mode under various scenarios.

**TABLE 19** Maintenance mode behavior under various scenarios

Operation with maintenance mode ENABLED	Interface administrative state with maintenance mode ENABLED	Final interface administrative state with maintenance mode DISABLED
Chassis enable/disable	Error message: "Not allowed"	N/A
Interface shut/no shut on edge ports	Current state is changed accordingly	State prior to maintenance mode is restored
ISL shut	Current state is changed accordingly	Current administrative state is preserved
Slot power off/on	Admin state in running-config is applied	State prior to maintenance mode is restored
ISSU/HA failover	Current state is maintained	State prior to maintenance mode is restored
Breakout/unbreakout/FlexPort	Default admin state (no shut) is applied to new interfaces	Default admin state is maintained for new interfaces
Insert new line card	Default admin state (no shut) is applied to new interfaces	Default admin state is maintained for new interfaces
Reboot in logical chassis cluster mode	Admin state in running-config is applied	State prior to maintenance mode is restored
Reboot in fabric cluster mode with copying running-config to startup-config	Admin state in startup-config is applied	State prior to maintenance mode is restored
Reboot in fabric cluster mode without copying running-config to startup-config	Admin state in startup-config is applied	N/A (maintenance mode config is lost)
Copying default-config to startup-config in logical chassis cluster mode	Default admin state is applied, maintenance mode is disabled	N/A
Copying default-config to startup-config, followed by reboot in fabric cluster mode	Default admin state is applied, maintenance mode is disabled	N/A

## Configuring maintenance mode

This task configures maintenance mode and verifies the configuration.

1. To enable maintenance mode, enter the **system-mode maintenance** command in RBridge ID configuration mode.

```
device# config terminal
device(config)# rbridge-id 1
device(config-rbridge-id-1)# system-mode maintenance
```

2. To confirm the configuration, you can use the **show vcs**, **show vcs detail**, and **show system** commands, as in the following respective examples.

```
device# show vcs
Config Mode      : Distributed
VCS Mode        : Logical Chassis
VCS ID          : 10
VCS GUID        : 6990c885-efa2-4b27-bb46-669d2d4d79f1
Total Number of Nodes      : 3
Rbridge-Id      WWN                Management IP   VCS Status     Fabric Status   HostName
-----
2                10:00:00:05:33:E6:BD:00           10.24.84.203   Online         Online          sw0
3                >10:00:00:05:33:65:63:64*         10.24.83.99    Maintenance    Online          sw0
4                10:00:00:27:F8:86:C2:45           10.24.83.97    Offline        Unknown         sw0
```

```
device# show vcs detail
Config Mode      : Distributed
VCS Mode        : Logical Chassis
```

```

VCS ID      : 149
VCS GUID    : 00000000000000000000000000000000
Virtual IP   : 20.0.0.1/24
Virtual IPV6 : 203::607/64
Associated rbridge-id : 2
Total Number of Nodes : 1
Nodes Disconnected from Cluster : 0
Cluster Condition : Good
Cluster Status : All Nodes Present in the Cluster
Node :1
  Serial Number : CPL2548J00Y
  Condition     : Good
  VCS Status    : Co-ordinator
  VCS Id       : 149
  Rbridge-Id   : 2*
  Co-ordinator  : YES
  WWN          : 10:00:00:27:F8:C3:C4:B2
  Switch MAC   : 00:27:F8:C3:C4:B2
  FCF MAC     : DE:AD:BE:EF:DE:AD
  Switch Type  : BR-VDX6740
  Internal IP  : 127.1.0.2
  Management IP : 10.37.18.150
  Fabric Status : Online
  Maintenance Mode : ON

```

```

device# show system
Stack MAC          : 00:05:33:e4:7f:2c

-- UNIT 0 --
Unit Name          : sw0
Switch Status      : Maintenance
Hardware Rev       : 1000.0
TengigabitEthernet Port(s) : 96
FortyGigabitEthernet Port(s) : 27
Up Time           : up 3 days 20:55
Current Time       : 06:50:54 GMT
NOS Version        : swrel_nos5.0.x_maint_150420_1403
Jumbo Capable     : yes

```

- Alternatively, use the **no** form of the command to disable maintenance mode and revert to the previous configuration status.

```
device(config-rbridge-id-1)# no system-mode maintenance
```

## Tunable SFP+ optics

Tunable SFP+ optics can be installed in 6740-10GbE ports, 6940-144S and 8770 with 48X10G Line cards.

The T-SFP+ interface defaults to a "no wavelength" state. When a Brocade device boots, the firmware sets the desired wavelength only if the wavelength is previously configured by the user. Else the brocade device boots with no-wavelength (default).

If you are installing a T-SFP+ in a 144S port, the T-SFP+ optic needs to be installed in both ends of the cable. The T-SFP+ at each end of the cable link must be configured at the same wavelength by setting them to the same channel on each device.

Failure to duplicate the channel setting may allow the link to come online, but the link behavior may be erratic.

If Brocade Network OS determines an error exceeding a specified limit, a RASLOG message event occurs and the port is taken offline.

When a T-SFP+ interface is installed it is very important that the interface is configured to the same channel (wavelength) at both ends.

Use the **show media tunable-optic-sfpp** command to determine the currently configured wavelength.

## Configuring tunable SFP+ optics

Perform the following task to configure a tunable SFP+ optic (T-SFP+) to a specific channel.

Repeat these steps for both devices on which the T-SFP+ is installed. You must set both devices to the same channel.

1. Select a channel for the T-SFP+ interface using the **show media tunable-optic-sfpp** command. There are 102 channels available.

```
device# show media tunable-optic-sfpp
command is show-media-tunable-optic-sfpp.
Channel   Wavelength
=====
1         1568.77
2         1568.36
3         1567.95
4         1567.54
5         1567.13
6         1566.72
7         1566.31
8         1565.90
9         1565.50
10        1565.09
(Output truncated for brevity.)
```

2. Enter global configuration mode.

```
device# configure terminal
```

3. Enter configuration mode for the interface for which the T-SFP+ is installed.

```
device(config)# interface tengigabitethernet 2/0/1
```

4. Use the **tunable-optics** command to set the channel for the interface.

```
device(conf-if-te-2/0/1)# tunable-optics sfpp channel 5
```

5. Confirm the channel configuration is online with the **show media optical-monitoring** command.

```
device(conf-if-te-2/0/1)# do show media optical-monitoring interface tengigabitethernet 2/0/1
N/A - Not Available.
N/S - Optical-monitoring Not Supported.
```

Port	Module	Supply	Channel	Frequency	Wavelength	Bias		
Channel		Temperature	Temp	Voltage	TX Power			
Current	RX Power	( C )	( mVolts )	( uWatts )	( GHz )	( nm )	( mAmps )	( uWatts )
Te 2/0/1	35	3314.1	0.1	0	0	0.000	0.0	

6. Confirm that the correct wavelength is configured by issuing the **show media interface** command.

```
device# show media interface tengigabitethernet 88/0/47
Interface      TenGigabitEthernet 88/0/47
Identifier     3      SFP
Connector      7      LC
Transceiver    0000000000000000
Name           id
Encoding       6
Baud Rate      99 (units 100 megabaud)
Length 9u      80 (units km)
Length 9u      255 (units 100 meters)
Length 50u     0 (units 10 meters)
Length 62.5u   0 (units 10 meters)
Length Cu      0 (units 1 meter)
Vendor Name    BROCADE
Vendor OUI     00:05:1e
Vendor PN      57-1000266-01
```

```

Vendor Rev      A
Wavelength     1528(units nm)
Options        065a Loss_of_Sig, Loss_of_Sig_Inverted
BR Max         10
BR Min         4
Serial No      AJJ21407557700C
Date Code      140223
Optical Monitor yes
Temperature    38 Centigrade
Voltage        3307.6 (mVolts)
Current        0.000 (mAmps)
TX Power       0.1 (uWatts)
RX Power       0.0 (uWatts)

```

## Tunable SFP+ optics channels

Tunable SFP+ optics are optional hardware that can be tuned to specific wavelengths and frequencies using pre-defined channels.

The following tables lists the frequency and wavelength assigned to channels for tunable SFP+ optic interfaces.

**TABLE 20** Supported wavelengths and channel numbers

Channel	Frequency (THz)	Wavelength (nm)
1	191.10	1568.77
2	191.15	1568.36
3	191.20	1567.95
4	191.25	1567.54
5	191.30	1567.13
6	191.35	1566.72
7	191.40	1566.31
8	191.45	1565.90
9	191.50	1565.50
10	191.55	1565.09
11	191.60	1564.68
12	191.65	1564.27
13	191.70	1563.86
14	191.75	1563.45
15	191.80	1563.05
16	191.85	1562.64
17	191.90	1562.23
18	191.95	1561.83
19	192.00	1561.42
20	192.05	1561.01
21	192.10	1560.61
22	192.15	1560.20
23	192.20	1559.79
24	192.25	1559.39
25	192.30	1558.98
26	192.35	1558.58
27	192.40	1558.17
28	192.45	1557.77

TABLE 20 Supported wavelengths and channel numbers (continued)

Channel	Frequency (THz)	Wavelength (nm)
29	192.50	1557.36
30	192.55	1556.96
31	192.60	1556.55
32	192.65	1556.15
33	192.70	1555.75
34	192.75	1555.34
35	192.80	1554.94
36	192.85	1554.54
37	192.90	1554.13
38	192.95	1553.73
39	193.00	1553.33
40	193.05	1552.93
41	193.10	1552.52
42	193.15	1552.12
43	193.20	1551.71
44	193.25	1551.32
45	193.30	1550.92
46	193.35	1550.52
47	193.40	1550.12
48	193.45	1549.72
49	193.50	1549.32
50	193.55	1548.91
51	193.60	1548.51
52	193.65	1548.11
53	193.70	1547.72
54	193.75	1547.32
55	193.80	1546.92
56	193.85	1546.52
57	193.90	1546.12
58	193.95	1545.72
59	194.00	1545.32
60	194.05	1544.92
61	194.10	1544.53
62	194.15	1544.13
63	194.20	1543.73
64	194.25	1543.33
65	194.30	1542.94
66	194.35	1542.54
67	194.40	1542.14
68	194.45	1541.75
69	194.50	1541.35

TABLE 20 Supported wavelengths and channel numbers (continued)

Channel	Frequency (THz)	Wavelength (nm)
70	194.55	1540.95
71	194.60	1540.56
72	194.65	1540.16
73	194.70	1539.77
74	194.75	1539.37
75	194.80	1538.98
76	194.85	1538.58
77	194.90	1538.19
78	194.95	1537.79
79	195.00	1537.40
80	195.05	1537.00
81	195.10	1536.61
82	195.15	1536.22
83	195.20	1535.82
84	195.25	1535.43
85	195.30	1535.04
86	195.35	1534.64
87	195.40	1534.25
88	195.45	1533.86
89	195.50	1533.47
90	195.55	1533.07
91	195.60	1532.68
92	195.65	1532.29
93	195.70	1531.90
94	195.75	1531.51
95	195.80	1531.12
96	195.85	1530.72
97	195.90	1530.33
98	195.95	1529.94
99	196.00	1529.55
100	196.05	1529.16
101	196.10	1528.77
102	196.15	1528.38

# Network Time Protocol

---

- [Network Time Protocol overview](#).....111
- [Configuring NTP](#).....111

## Network Time Protocol overview

Network Time Protocol (NTP) maintains uniform time across all switches in a network. The NTP commands support the configuration of an external time server to maintain synchronization between all local clocks in a network.

To keep the time in your network current, it is recommended that each switch have its time synchronized with at least one external NTP server. External NTP servers should be synchronized among themselves in order to maintain fabric-wide time synchronization.

All switches in the fabric maintain the current clock server value in nonvolatile memory. By default, this value is the local clock server of the switch.

## Date and time settings

Brocade switches maintain the current date and time inside a battery-backed real-time clock (RTC) circuit. Date and time are used for logging events. Switch operation does not depend on the date and time; a switch with incorrect date and time settings can function correctly. However, because the date and time are used for logging, error detection, and troubleshooting, you should set them correctly.

## Time zone settings

You can set the time zone by specifying a geographic region and city by name. You can choose one of the following regions: Africa, America, Pacific, Europe, Antarctica, Arctic, Asia, Australia, Atlantic, and Indian.

The time zone setting has the following characteristics:

- The setting automatically adjusts for Daylight Savings Time.
- Changing the time zone on a switch updates the local time zone setup and is reflected in local time calculations.
- By default, all switches are in the Greenwich Mean Time (GMT) time zone (0,0). If all switches in a fabric are in one time zone, it is possible for you to keep the time zone setup at the default setting.
- System services that have already started will reflect the time zone changes only after the next reboot.
- Time zone settings persist across failover for high availability.
- Time zone settings are not affected by NTP server synchronization.

## Configuring NTP

The following sections discuss how to correctly configure the Network Time Protocol for Brocade switches.

## Configuration considerations for NTP

Network time synchronization is guaranteed only when a common external time server is used by all switches. If you are in VCS mode, when an **ntp server** command is invoked on one switch in a cluster, the configuration is applied to all switches in the cluster.

The **ntp server** command accepts up to five server addresses in IPv4 or IPv6 format. When you configure multiple NTP server addresses, the **ntp server** command sets the first obtainable address as the active NTP server. If there are no reachable time servers, then the local switch time is the default time until a new active time server is configured.

## Setting the date and time

The **clock set** command sets the local clock date and time. Valid date and time values must be in the range between January 1, 1970 and January 19, 2038. If a time zone is not configured, the time zone defaults to Greenwich Mean Time (GMT). If an active NTP server is configured for the switch, it overrides the local time settings.

Enter the **clock set CCYY-MM-DDTHH:MM:SS** command.

The variables represent the following values:

- *CCYY* specifies the year; the valid range is 1970 through 2038.
- *MM* specifies the month; the valid range is 01 through 12.
- *DD* specifies the day; the valid range is 01 through 31.
- *HH* specifies the hour; the valid range is 00 through 23.
- *MM* specifies the minutes; the valid range is 00 through 59.
- *SS* specifies the seconds; the valid range is 00 through 59.

If you are in VCS mode, setting the time and date is done using the RBridge ID of the node.

Here is an example of setting and displaying the date and time in VCS mode:

```
switch# clock set 2013-06-06T12:15:00 rbridge-id all
switch# show clock
rbridge-id all: 2013-06-06 12:15:05 Etc/GMT+0
```

## Setting the time zone

Use the **clock timezone** command to set the time zone for a switch. You must use the command for all switches for which a time zone must be set. However, you only need to set the time zone once on each switch, because the value is written to nonvolatile memory.

Setting the time and date can be done in Privileged EXEC mode by using the RBridge ID of the node. (Setting the date and time can also be done in RBridge ID configuration mode, but must be done on a per-node basis in this mode.) Refer to the **clock timezone** command in each mode in the *Network OS Command Reference*.

Refer to the *Network OS Troubleshooting Guide* for a complete list of configurable regions and cities.

Enter the **clock timezone region/city** command.

```
switch# clock timezone America/Los_Angeles rbridge-id all
```

### NOTE

Upgrade considerations: The existing timezone of the system is retained after a firmware upgrade, and it will be updated in configuration settings.

General downgrade considerations: The existing timezone of the system is retained after firmware downgrade and the respective entry will be removed from configuration settings.

Russian time zone downgrade considerations: Because of changes to the Russian time zone in NOS 6.0.1, if you want to downgrade to a release prior to 6.0.1 and you have Russian time zones configured, be aware that:

- In logical chassis cluster mode, the downgrade is blocked if running-config includes the new Russian time zone configuration.
- In fabric cluster mode, the downgrade is blocked if startup-config include the new time Russian time zone configuration.



## Displaying the current local clock and time zone

The **show clock** command returns the local time, date, and time zone.

### NOTE

This command is currently supported on the local switch.

This example shows the local switch clock time:

```
switch# show clock
rbridge-id 1: 2012-05-04 16:01:51 America/Los Angeles
```

This example shows the clock time for all switches in the cluster (logical chassis cluster mode only):

```
switch# show clock rbridge-id all
rbridge-id 1: 2013-06-06 12:15:05 Etc/GMT+0
rbridge-id 5: 2013-06-06 12:15:05 Etc/GMT+0
rbridge-id 10: 2013-06-06 12:15:05 Etc/GMT+0
```

This example shows the clock time for the switch with rbridge-id 16:

```
switch# show clock rbridge-id 16
rbridge-id 16: 2012-05-04 18:18:51 America/Los Angeles
```

## Removing the time zone setting

Use the **no clock timezone** command to remove the time zone setting for the local clock. This operation returns the local time zone to the default value (GMT). When using the **no** operand, you do not need to reference a timezone setting.

Enter the **no clock timezone** command.

```
switch# no clock timezone rbridge-id 5
```

### NOTE

The **clock timezone** command can be run in privileged EXEC mode, as shown in the previous example, or in RBridge ID configuration mode. Refer to the *Network OS Command Reference* for descriptions of this command in each of these modes.

## Synchronizing the local time with an external source

Use the **ntp server** command to synchronize the local switch time with an NTP server. You can configure up to five IP address. At least one IP address in the list must be a reachable, configured NTP server or the request will fail.

The following example synchronizes the time on the local switch with the ntp server at 192.168.10.1.

Enter the **ntp server ip\_address** command.

```
switch(config)# ntp server 192.168.10.1
```

## Displaying the active NTP server

Use the **show ntp status** command to display the current active NTP server IP address. If an NTP server is not configured or the server is unreachable, the output displays LOCL (for local switch time). Otherwise, the command displays the NTP server IP address. The command displays the local NTP server configuration only.

If the RBridge ID parameter is not provided, status results default to the local switch. If **rbridge-id all** is specified, the command displays the status for all switches in the cluster. If the RBridge ID is specified, the command displays that node's NTP status.

This example shows the local switch NTP status when an NTP server is not configured:

```
switch# show ntp status
rbridge-id 1: active ntp server is LOCL
```

This example shows the configured NTP server:

```
switch# show ntp status
rbridge-id 1: active ntp server is 10.31.2.81
```

This example shows NTP status for all switches in a cluster.

```
switch# show ntp status rbridge-id all
rbridge-id 7: active ntp server is LOCL
```

## Removing an NTP server IP address

To remove an NTP server IP address from the list of server IP addresses on a switch, enter **no ntp server** followed by the server IP address.

The following example removes the NTP server at 192.168.10.1 from the local server IP address database.

```
switch(config)# no ntp server 192.168.10.1
switch# show ntp status
rbridge-id 1: active ntp server is LOCL
```

### IMPORTANT



At least one IP address in the remaining list must be for a reachable and configured NTP server; if there is not one the remove request will fail.

## Authenticating NTP

You can create an authentication key for the purpose of authenticating an external NTP server .

You use the **ntp authentication-key** command to configure a key identifier and secret key strings, which are added to the database. The key is shared by the client (switch) and an external NTP server. You then associate the key to an NTP server by using the **ntp server** command.

For more information, refer to the **ntp authentication-key** and **ntp server** commands in the *Network OS Command Reference*.

# Configuration Management

- Configuration management overview.....115
- Displaying configurations.....116
- Saving configuration changes.....117
- Backing up configurations.....118
- Configuration restoration.....119
- Managing configurations on a modular chassis.....119
- Managing configurations in Brocade VCS Fabric mode.....120
- Rejoining an offline node to a logical chassis cluster.....121
- Using default configuration in logical chassis cluster to avoid segmentation issues.....122
- Managing flash files.....122

## Configuration management overview

Maintaining consistent configuration settings among switches in the same fabric is an important part of switch management and minimizes fabric disruptions. As part of standard maintenance procedures, it is recommended that you back up all important configuration data for every switch on an external host for emergency reference.

Typical configuration management tasks include the following actions:

- Saving the running configuration to the startup configuration file ([Saving configuration changes](#) on page 117).
- Uploading the configuration files to a remote location ([Backing up configurations](#) on page 118).
- Restoring a configuration file from a remote archive ([Configuration restoration](#) on page 119).
- Archiving configuration files for all your switches to a remote location ([Managing configurations in Brocade VCS Fabric mode](#) on page 120).
- Downloading a configuration file from a remote location to multiple switches ([Managing configurations in Brocade VCS Fabric mode](#) on page 120).

## Configuration file types

Brocade Network OS supports three types of configuration files. The table below lists the standard configuration files and their functions.

**TABLE 21** Standard switch configuration files

Configuration file	Description
<b>Default configuration</b> <ul style="list-style-type: none"><li>• defaultconfig.novcs</li><li>• defaultconfig.vcs</li></ul>	Part of the Network OS firmware package. The default configuration is applied, if no customized configuration is available.
<b>Startup configuration</b> <ul style="list-style-type: none"><li>• startup-config</li></ul>	Configuration effective on startup and after reboot.
<b>Running configuration</b> <ul style="list-style-type: none"><li>• running-config</li></ul>	Current configuration active on the switch. Whenever you make a configuration change, it is written to the running configuration. For fabric cluster mode, the running configuration does not persist across reboot, unless you copy it to the startup configuration.  However, when the switch is in logical chassis cluster mode, the running-config file is saved automatically and it does not need to be copied.

Configuration management follows a transaction model. When you boot up a switch for the first time, the running configuration is identical to the startup configuration. As you configure the switch, the changes are written to the running configuration. To save the changes, you must save the currently effective configuration (the running configuration) as the startup configuration. When the switch reboots, the configuration changes become effective.

## Default configuration

Default configuration files are part of the Network OS firmware package and are automatically applied to the startup configuration under the following conditions:

- When the switch boots up for the first time and no customized configuration is available.
- When you restore the default configuration.

You cannot remove, rename, or change the default configuration.

## Startup configuration

### NOTE

There is no startup configuration for logical chassis cluster mode. Switches in a logical chassis cluster always preserve their running configuration.

The startup configuration is persistent. It is applied when the system reboots.

- When the switch boots up for the first time, the switch uses the default configuration as the startup configuration, depending on the mode.
- The startup configuration always matches the current Brocade VCS Fabric mode. It is deleted when you change modes, unless you make a backup copy.
- When you make configuration changes to the running configuration and save the changes to the startup configuration with the **copy** command, the running configuration becomes the startup configuration.

## Running configuration

The configuration currently effective on the switch is referred to as the running configuration. Any configuration change you make while the switch is online is made to the running configuration.

- The running configuration is nonpersistent.
- To save configuration changes, you must copy the running configuration to the startup configuration. If you are not sure about the changes, you can copy the changes to a file, and apply the changes later.

## Displaying configurations

The following examples illustrate how to display the default, startup, and running configurations, respectively.

### Displaying the default configuration

To display the default configuration, enter the **show file filename** command in privileged EXEC mode.

```
switch# show file defaultconfig.novcs
switch# show file defaultconfig.vcs
```

## Displaying the startup configuration

To display the contents of the startup configuration, enter the **show startup-config** command in privileged EXEC mode.

```
switch# show startup-config
```

## Displaying the running configuration

To display the contents of the running configuration, enter the **show running-config** command in the privileged EXEC mode.

```
switch# show running-config
```

## Saving configuration changes

Configuration changes are nonpersistent and are lost on reboot unless you save them permanently. You have two options for saving configuration changes:

- Copy the running configuration to the startup configuration. The changes become effective upon reboot.
- Copy the running configuration to a file, and apply it at some later date.

### NOTE

Always make a backup copy of your running configuration before you upgrade or downgrade the firmware.

## Saving the running configuration

To save the configuration changes you made, copy the running configuration to the startup configuration. The next time the switch reboots, it uses the startup configuration and the changes you made earlier become effective.

### NOTE

When the switch is in logical chassis cluster mode, the running-config file is saved automatically and it does not need to be copied.

Enter the **copy running-config startup-config** command in privileged EXEC mode.

```
switch# copy running-config startup-config
copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
```

## Saving the running configuration to a file

If you want to save the changes you made to the configuration, but you do not want the changes to take effect when the switch reboots, you can save the running configuration to a file. You can apply the changes at some later time.

1. Enter the **copy running-config file** command in privileged EXEC mode. Specify the file name as the file URL.

```
switch# copy running-config flash://myconfig
```

2. Verify the transaction by listing the directory contents.

```
switch# dir
total 32
drwxr-xr-x  2 root    sys      4096 Feb 17 17:50 .
drwxr-xr-x  3 root    root     4096 Jan  1 1970 ..
-rwxr-xr-x  1 root    sys       417 Oct 12 2010 defaultconfig.novcs
-rwxr-xr-x  1 root    sys       697 Oct 12 2010 defaultconfig.vcs
-rw-r--r--  1 root    root     6777 Feb 17 17:50 myconfig
-rw-r--r--  1 root    root     6800 Feb 13 00:37 startup-config
```

## Applying previously saved configuration changes

When you are ready to apply the configuration changes you previously saved to a file, copy the file (*myconfig* in the example) to the startup configuration. The changes take effect after the switch reboots.

Enter the **copy filename startup-config** command in privileged EXEC mode. Specify the file name as the file URL.

```
switch# copy flash://myconfig startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
```

## Backing up configurations

Always keep a backup copy of your configuration files, so you can restore the configuration in the event the configuration is lost or you make unintentional changes.

### NOTE

This operation is not supported in logical chassis cluster mode, because the running-config will be auto-synced to the startup-config.

The following recommendations apply:

- Keep backup copies of the startup configuration for all switches in the fabric.
- Upload the configuration backup copies to an external host or to an attached Brocade-branded USB device.
- Avoid copying configuration files from one switch to another. Instead restore the switch configuration files from the backup copy.

## Uploading the startup configuration to an external host

Enter the **copy startup-config destination\_file** command in privileged EXEC mode.

In the following example, the startup configuration is copied to a file on a remote server by means of FTP.

```
switch# copy startup-config ftp://admin:*****@122.34.98.133//archive/startup-config_vdx24-08_20101010
```

## Backing up the startup configuration to a USB device

When you make a backup copy of a configuration file on an attached USB device, the destination file is the file URL on the USB device. You do not need to specify the target directory. The file is automatically recognized as a configuration file and stored in the default configuration directory.

1. Enable the USB device.

```
switch# usb on
USB storage enabled
```

2. Enter the **copy startup-config destination\_file** command in privileged EXEC mode.

```
switch# copy startup-config usb://startup-config_vdx24-08_20101010
```

## Configuration restoration

Restoring a configuration involves overwriting a given configuration file on the switch by downloading an archived backup copy from an external host or from an attached USB device.

A typical scenario for configuration restoration is:

- [Restoring the default configuration](#) on page 119.

All interfaces remain online. The following parameters are unaffected:

- Interface management IP address
- Software feature licenses installed on the switch
- Virtual IP address

### NOTE

Configuration files that were created using Brocade Network OS 2.x should not be loaded onto a system running Brocade Network OS 3.x or later. The ACL and VLAN configuration information has changed in Brocade Network OS 3.x or later, and the affected lines of configuration are skipped when loading a Brocade Network OS 2.x configuration file.

## Restoring the default configuration

This restoration procedure resets the configuration to the factory defaults. The default configuration files are always present on the switch and can be restored with the **copy** command.

To restore the default configuration, perform the following procedure in privileged EXEC mode.

1. Enter the **copy *source\_file destination\_file*** command to overwrite the startup configuration with the default configuration.

```
switch# copy default-config startup-config
```

2. Confirm that you want to make the change by entering Y when prompted.

```
This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
```

3. Reboot the switch.

```
switch# reload system
```

## Managing configurations on a modular chassis

### NOTE

When the switch is in logical chassis cluster mode, the running-config file is saved automatically and does not need to be copied. There is no startup configuration for logical chassis cluster mode; therefore, the information about startup configuration does not apply to logical chassis cluster mode.

The configuration data on a modular chassis are managed in a distributed fashion. The Brocade VDX 8770-4 and VDX 8770-8 chassis maintain two types of configuration data, global configuration parameters and slot configuration parameters. The global configuration, such as the VLAN configuration, applies to the entire chassis. The slot configuration includes specific parameters that apply only to the line cards.

The startup configuration is maintained at the chassis level and includes both chassis-wide and slot-specific configuration parameters.

## Managing configurations on line cards

When an line card (interface module) boots up in a slot which was never occupied previously or is not configured, the module type is automatically saved in the configuration database. The type configuration associated with a given slot persists in the database even after the line card is physically removed, powered off, or faulted. This mechanism ensures that all configuration data associated with a given slot is automatically preserved across reboots or hot swaps with the same type of line card.

If you insert an line card in a slot that was previously occupied by a module of a different type, the line card will be faulted with a "type mismatch" error. Before you replace an line card with a different type, you must clear the existing type configuration from the database. Refer to [Replacing a line card](#) on page 86 for more information.

### NOTE

The line card configuration is non-persistent. You must issue the **copy running-config startup-config** command after the line card comes online. Otherwise, all configuration data associated with the slot along with line module type will be lost after a chassis reboot.

## Managing configurations across redundant management modules

In modular switches with redundant management modules, the VCS configuration, the startup configuration, and the startup database are synchronized and shared between the two management modules. The initial configuration synchronization occurs when the system boots up. After the initial synchronization has been completed successfully, synchronization can be triggered during the following events:

- When a failover occurs from the active management module to the standby management module. Unsaved configuration changes made on the active management module are lost after a failover. Issue the **copy running-config startup-config** command on the active management module to preserve the running configuration across a management module failover.
- When you insert a standby management module into a chassis after the active management module is already fully initialized.
- When you change the startup configuration by issuing the **copy running-config startup-config** command on the active management module.
- When you restore the default configuration by issuing the **copy default-config startup-config** command on the active management module.
- When you change the VCS configuration (VCS mode, RBridge ID, or VCS ID), the configuration change is synchronized with the standby management module and saved persistently. This event triggers a chassis reboot after the synchronization is complete.
- When you initiate a firmware download. Refer to [Configuration Management](#) on page 115 for more information.

## Managing configurations in Brocade VCS Fabric mode

With the exception of a few parameters, configuration changes you make to a single switch in a Brocade VCS Fabric are not automatically distributed. When configuring Ethernet fabric parameters and software features on multiple switches, you must configure each switch individually. To simplify the procedure, you can upload a configuration file from one switch and download it to the other switches in the fabric, provided the switches are of the same type.

### NOTE

The switches must be of the same model to share a configuration file. For example, downloading a configuration file from a Brocade VDX 6740-48 to a Brocade VDX 6740-64 or to a switch with a different firmware version may cause the switch to misapply the configuration and lead to unpredictable behavior.

To determine the switch type, issue the **show system** command. To map the switch type to the Brocade switch model name, refer to [Switch types](#) on page 56.



If you need to reset affected switches, restore the default configuration as described in [Restoring the default configuration](#) on page 119.

## Automatic distribution of configuration parameters

A few configuration parameters are fabric-wide in fabric cluster mode. This means they are automatically distributed to all switches in a VCS fabric when you configure one or more of these parameters on a single RBridge that is part of a VCS fabric. These parameters include the following:

- Zoning configuration
- vCenter parameters
- Virtual IP address

### NOTE

In logical chassis cluster mode, all configuration is automatically distributed.

The **show running configuration** command displays the same configuration for these features on all RBridges in the VCS fabric. Copy operations from any RBridge include all fabric-wide configuration parameters.

## Downloading a configuration to multiple switches

### NOTE

This section does not apply to logical chassis cluster mode because, in that mode, configuration is automatically distributed.

1. Configure one switch.
2. Copy the running configuration to the startup configuration as described in [Saving the running configuration](#) on page 117.
3. Upload the configuration to an external host ([Uploading the startup configuration to an external host](#) on page 118) or to an attached USB device as described in [Backing up the startup configuration to a USB device](#) on page 118.
4. Download the configuration file to each of the target switches. Refer to [Configuration restoration](#) on page 119 for more information.

## Rejoining an offline node to a logical chassis cluster

If a node goes into offline state, and configuration changes are made to online nodes while the cluster is in a degraded state, database mismatches can occur when the offline node tries to rejoin the cluster.

Situations that can cause a node to go offline include:

- ISLs are shutdown, isolating a node from the fabric and cluster.
- A node reboots.

The following list describes possible scenarios that can occur when an offline node tries to rejoin its cluster, and what actions, if any, you must take. For more information about commands that are referenced, refer to the *Network OS Command Reference*.

- If local-only configurations have been added, updated, or deleted for online nodes after another node has temporarily left the cluster, the offline node automatically rejoins the cluster. Any non-default configurations specific to the rejoining node are then pushed back to the cluster configuration. If the rejoining node has the default configuration, and if no local-only configuration changes were made while this node was offline, then the cluster's configuration for the rejoining node is pushed onto the rejoining node.

- If the offline node has local-only configuration changes and its global configuration is non-default and matches the global configuration of the cluster, then the offline node is allowed to rejoin the cluster. The local-only configuration changes that were made while the node was offline are preserved.
- If global configurations have been added, updated, or deleted after another node has temporarily left the cluster, the global configuration differences between the cluster and the rejoining node result in a configuration database mismatch and node segmentation. To rejoin the cluster, issue the **copy default-config startup-config** on the segmented node.
- If the rejoining node's global configuration is the default configuration, and both of the following are true: 1) local-only configuration changes have been made to the rejoining node while it was offline, and 2) the cluster contains a different set of local configurations for the rejoining node, then a configuration database mismatch occurs. This situation can occur if the user issues a **copy default to start** command on a segmented node and issues local-only configurations on the segmented node before it rejoins the cluster. To rejoin the cluster, issue the **copy default to startup** command on the segmented node or cluster island.

The following table lists commands that change a local configuration for a node but also affect the global configuration. If these commands are run on online nodes in the cluster, be aware that global configuration in the cluster will also change.

**TABLE 22** Local-configuration commands that affect global configuration

Command (Local Configuration)	Description
<b>flexport</b> <RBridge-ID/slot/port>, followed by the <b>type fibre-channel</b> command from the flexport rbridge-id/slot/port prompt, changes the global configuration.	Done in Hardware configuration mode, this command, which converts an Ethernet interface to a Fibre-Channel interface, can cause global configuration changes because the Ethernet interface affects L2Sys, SPAN, IGMPs, and MLD configuration settings.
<b>vrf</b> <name>	Done in RBridge-ID configuration mode, the creation of a VRF on an RBridge is a local-only VRF configuration exception and also changes the global configuration.

## Using default configuration in logical chassis cluster to avoid segmentation issues

Using a command called **default-config enable** allows a node to rejoin a logical chassis cluster by obtaining the configuration of the principal node in the cluster.

Enabling this feature can eliminate the following segmentation issues:

- A node rebooting while a global configuration change could not be applied.
- ISL connectivity to the primary node going down while configuration is in progress.

Brocade recommends not enabling this feature on *every* node (especially on core nodes) in the cluster.

The following restrictions apply:

- This command cannot be used on the principal node of the logical chassis cluster.
- Principal priority cannot be set on a node which has this feature enabled.

For information on how to use this command, refer to the **default-config enable** command in the *Network OS Command Reference*.

## Managing flash files

Brocade Network OS provides a set of tools for removing, renaming, and displaying files you create in the switch flash memory. You can use the display commands with any file, including the system configuration files. The **rename** and **delete** commands only apply to copies of configuration files you create in the flash memory. You cannot rename or delete any of the system configuration files.

## Listing the contents of the flash memory

To list the contents of the flash memory, enter the **dir** command in privileged EXEC mode.

```
switch# dir
drwxr-xr-x  2 root    sys      4096 Feb 13 00:39 .
drwxr-xr-x  3 root    root     4096 Jan  1 1970 ..
-rwxr-xr-x  1 root    sys       417 Oct 12 2010 defaultconfig.novcs
-rwxr-xr-x  1 root    sys       697 Oct 12 2010 defaultconfig.vcs
-rw-r--r--  1 root    root     6800 Feb 13 00:37 startup-config
```

## Deleting a file from the flash memory

To delete a file from the flash memory, enter the **delete file** command in privileged EXEC mode.

```
switch# delete myconfig
```

## Renaming a flash memory file

To rename a file in the flash memory, enter the **rename source\_file destination\_file** command in privileged EXEC mode.

```
switch# rename myconfig myconfig_20101010
```

## Viewing the contents of a file in the flash memory

To investigate the contents of a file in the flash memory, enter the **show file file** command in privileged EXEC mode.

```
switch# show file defaultconfig.novcs
!
no protocol spanning-tree
!
vlan dot1q tag native
!
cee-map default
remap fabric-priority priority 0
remap lossless-priority priority 0
priority-group-table 1 weight 40 pfc on
priority-group-table 2 weight 60 pfc off
priority-group-table 15.0 pfc off
priority-table 2 2 2 1 2 2 2 15.0
!
interface Vlan 1
shutdown
!
port-profile default
vlan-profile
switchport
switchport mode trunk
switchport trunk allowed vlan all
!
protocol lldp
!
end
!
```

### NOTE

To display the contents of the running configuration, use the **show running-config** command. To display the contents of the startup configuration, use the **show startup-config** command.



# SNMP

---

- [Simple Network Management Protocol overview](#).....125
- [SNMP configuration](#).....126

## Simple Network Management Protocol overview

Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks. SNMP protocols are application layer protocols. Using SNMP, devices within a network send messages, called protocol data units (PDUs), to different parts of a network. Network management using SNMP requires three components:

- SNMP Manager
- SNMP Agent
- Management Information Base (MIB)

### SNMP Manager

The SNMP Manager can communicate to the devices within a network using the SNMP protocol. Typically, SNMP Managers are network management systems (NMS) that manage networks by monitoring the network parameters, and optionally, setting parameters in managed devices. Normally, the SNMP Manager sends read requests to the devices that host the SNMP Agent, to which the SNMP Agent responds with the requested data. In some cases, the managed devices can initiate the communication, and send data to the SNMP Manager using asynchronous events called traps.

### SNMP Agent

The SNMP agent is a software that resides in the managed devices in the network, and collects data from these devices. Each device hosts an SNMP Agent. The SNMP Agent stores the data, and sends these when requested by an SNMP Manager. In addition, the Agent can asynchronously alert the SNMP Manager about events, by using special PDUs called traps.

### Management Information Base (MIB)

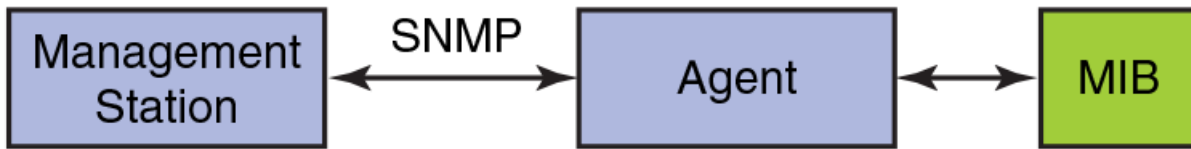
SNMP Agents in the managed devices store the data about these devices in a database called Management Information Base (MIB). The MIB is a hierarchical database, which is structured on the standard specified in the RFC 2578 [Structure of Management Information Version 2 (SMIv2)].

The MIB is a database of objects that can be used by a network management system to manage and monitor devices on the network. The MIB can be retrieved by a network management system that uses SNMP. The MIB structure determines the scope of management access allowed by a device. By using SNMP, a manager application can issue read or write operations within the scope of the MIB.

### Basic SNMP operation

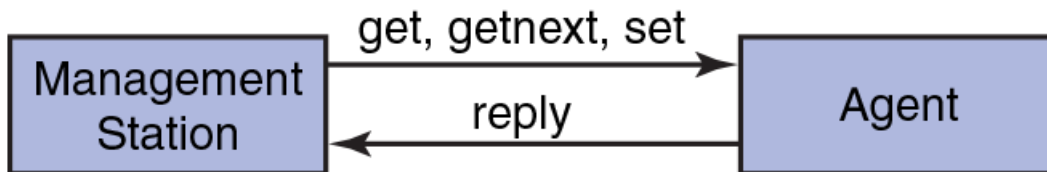
Every Brocade device carries an *agent* and management information base (MIB), as shown in the next figure. The agent accesses information about a device and makes it available to an SNMP network management station.

FIGURE 19 SNMP structure



When active, the management station can "get" information or "set" information when it queries an agent. SNMP commands, such as **get**, **set**, **getnext**, and **getresponse**, are sent from the management station, and the agent replies once the value is obtained or modified as shown in the next figure. Agents use variables to report such data as the number of bytes and packets in and out of the device, or the number of broadcast messages sent and received. These variables are also known as managed objects. All managed objects are contained in the MIB.

FIGURE 20 SNMP query



The management station can also receive *traps*, unsolicited messages from the switch agent if an unusual event occurs as shown in the next figure.

FIGURE 21 SNMP trap



The agent can receive queries from one or more management stations and can send traps to up to six management stations.

## SNMP configuration

The following sections discuss configuring the Simple Network Management Protocol on Brocade devices. This includes configuring SNMP community strings, SNMP server hosts, SNMP server contexts, password encryption for SNMPv3 users, and displaying SNMP configurations.

**ATTENTION**

The SNMP default configurations, such as community string, user name, community, group, view configuration, and so on, have been removed, because of a security risk. The **show running-config snmp-server** command displays only system parameters during startup. You can configure the appropriate SNMP attributes by using a variety of **snmp-server** commands. (This does not apply to the Brocade VDX 2746, which displays both system and default user SNMP configurations.)

Note the following:

- After an upgrade to Network OS6.0.0 or later, the default SNMP configuration from previous releases is removed only if the **copy default-config startup-config** command is issued before the upgrade. Otherwise, the running configuration is not changed.
- There is no change in the behavior of the upgrade from the running configuration to the startup configuration.
- Following a netinstall to Network OS6.0.0 or later, or a reboot when the default configuration is copied to the startup configuration, the following SNMP configuration appears, with previous default configurations removed:

```
device#show running-config snmp-server

snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server enable trap
```

## Configuring SNMP community strings

SNMP versions 1 and 2c use community strings to restrict access to the switch. There is support for a total of 256 SNMP communities.

### Adding an SNMP community string

The **snmp-server community** command sets the community string and associates it with the user-defined group to restrict the access of MIBs for SNMPv1 and SNMPv2c requests. You execute this command in global configuration mode.

1. Enter the **configure** command.

```
switch# configure
```

2. Enter the **snmp-server community** command.

```
switch(config)# snmp-server community comm1 groupname accGroup1
switch(config)#
```

When creating a new community string without specifying a group name, there is no group name associated with the community string. You must associate the community string with any nonexisting or existing group name to be able to contact the switch using SNMPv1/v2c.

The following example also applies an IPv4 ACL and an IPv6 ACL.

```
switch(config)# snmp-server community comm1 groupname accGroup1 ipv4-acl standV4ACL1 ipv6-acl
standV6ACL1
switch(config)#
```

**NOTE**

For the entire flow of implementing SNMP ACLs, refer to [Implementation flow of ACLs under SNMP](#) on page 134.

**NOTE**

The Brocade VDX 2746 supports only the default group names (admin and user).

## Removing an SNMP community string

The following example removes the community string "public" and its associated group name "user".

1. Enter the **configure** command.
2. Enter the **no snmp-server community *string*** command.

```
switch(config)# no snmp-server community public
```

The following example removes the associated IPv4 and IPv6 ACLs from the SNMP community.

```
switch(config)# no snmp-server community public ipv4-acl
switch(config)# no snmp-server community public ipv6-acl
```

## Configuring SNMP server hosts

The **snmp-server host** command sets the trap destination IP addresses, SNMP version, community string for SNMPv1 and SNMPv2c, the destination port for the SNMP server host, the severity level, and the SNMP communication through default VRF (default-vrf) or management VRF (mgmt-vrf) or user-defined VRF.

To configure SNMP trap hosts associated with community strings, you must create the community string using the **snmp-server community** command before configuring the host.

The SNMP agent supports six trap-recipient severity levels. The default value for each attribute is as follows: host = 0.0.0.0; udp-port = 162; severity-level = none. The length of the community string must be from 2 through 64 characters.

### Setting the SNMP server host

The **snmp-server host** command configures a SNMP host by associating with the SNMP users. You execute this command in global configuration mode.

Refer to the *Network OS Command Reference* for complete descriptions of all the SNMP server host options.

1. Execute the **configure terminal** command to enter global configuration mode.
2. Execute the **snmp-server host** to configure the SNMP server host.

The following example sets up "commaccess" as a community string and sets 10.32.147.6 as a trap recipient with SNMPv2c on target port 162, with default-vrf.

```
switch(config)# snmp-server host 10.32.147.6 commaccess version 2c udp-port 162 severity warning use-
vrf default-vrf
```

### Removing the SNMP server host

The **no snmp-server host *host* community-string *string*** command removes the SNMP server host from the switch configuration.

## Configuring the SNMP system group

The following tasks allow you to configure the system contact and system location objects for the SNMP system group.

### Setting the SNMP server contact

Use the **snmp-server contact** command to set the SNMP server contact string. The default contact string is "Field Support." The number of characters allowed is from 4 through 255.

1. Enter the **configure** command.



2. Enter the **snmp-server contact** *string* command.

```
switch(config)# snmp-server contact "Operator 12345"
```

The example changes the default contact string to "Operator 12345." You must enclose the text in double quotes if the text contains spaces.

### Removing the SNMP server contact

The **no snmp-server contact** *string* command restores the default contact information (Field Support).

### Setting the SNMP server location

Use the **snmp-server location** command to set the SNMP server location string. The default SNMP server location string is "End User Premise." The number of characters allowed is from 4 through 255.

1. Enter the **configure** command.
2. Enter the **snmp-server location** *string* command.

```
switch(config)# snmp-server location "Building 3 Room 214"
```

3. Enter the **no snmp-server location** command to remove the location.

The example changes the default location string to "Building 3 Room 214." You must enclose the text in double quotes if the text contains spaces.

### Setting the SNMP server description

Use the **snmp-server sys-descr** command to set the SNMP server description string. The default SNMP server description string is "Brocade-VDX-VCS <vcsid>." The number of characters allowed is from 4 through 255.

1. Enter the **configure** command.
2. Enter the **snmp-server sys-descr** *string* command.

```
switch(config)# snmp-server sys-descr "Brocade-VDX Test Bed"
```

3. Enter the **no snmp-server sys-descr** command to remove the location.

The example changes the default location string to "Brocade-VDX Test Bed." You must enclose the text in double quotes if the text contains spaces.

## Configuring multiple SNMP server context to VRF mapping

A single SNMP agent can be supported by multiple instances of the same MIB module by mapping the context name to a virtual routing and forwarding (VRF) instance created within the switch. Each VRF is mapped with a specific key called context name. The context name is used to identify the VRF and fetch the MIB details of the mapped VRF from the underlying modules. For example, the OSPF-MIB by default returns the queried OSPF-MIB object values pertaining to the default VRF (default-vrf). The user input will vary for different SNMP versions. In case of snmp v1 and v2c, we have to map the context with the community by using the command "snmp-server mib community-map". The SNMP agent supports 256 contexts to support context-to-VRF mapping.

The mapping of the community to context and context to VRF is given in the following examples.

1. Create a community "public" with Groupname "admin".
  - Enter the **configure** command.

```
switch(config)# snmp-server community public groupname admin
```

2. Create a context and map with VRF. The VRF can be default-vrf or user defined vrf.

- Enter the **configure** command.
- Enter the **snmp-server context** *context\_name* **vrf** *vrf-name* command.

```
switch(config)# snmp-server context mycontext vrf myvrf
```

3. Map the community to context.

- Enter the **configure** command.

```
switch(config)# snmp-server mib community-map public context mycontext
```

In the above example, the community "public" is mapped with the context "mycontext" and the context in turn mapped with the "myvrf". To fetch the OSPF MIB-objects values belonging to the "myvrf", use community public for snmpv1 and v2c query.

Perform the following steps to set the SNMP server context, using the **snmp-server context** command and to map the context name in a SNMPv3 packet's protocol data unit (PDU) to the name of a VPN routing and forwarding (VRF) instance. The context-to-VRF mapping is one-to-one and is applicable to all SNMP versions. Only one context is allowed per VRF instance. For SNMPv3, it is enough to map the context with VRF. The snmpv3 request PDU itself will have the provision for context name as input.

4. Create an user "snmpuser1" with group name "admin".

- Enter the **configure** command.

```
switch(config)# snmp-server user snmpuser1 auth md5 auth-password 123456789 priv DES priv-  
password 123456789 groupname admin
```

5. Map the context mycontext with myvrf.

- Enter the **configure** command.
- Enter the **snmp-server context** *context\_name* **vrf** *vrf-name* command.

```
switch(config)# switch(config)# snmp-server context mycontext vrf myvrf
```

Perform snmpv3 query with user and context name with the corresponding credentials. For group name information, refer to [Configuring SNMP server groups](#) on page 131.

## Configuring SNMP server views

SNMP views are named groups of MIB objects that can be associated with user accounts to allow limited access for viewing and modifying the SNMP statistics and system configuration. With SNMP views user can create or remove the access to MIB object that need to be included or excluded from viewing.

SNMP views reference MIB objects using object names. It represents the hierarchical location of the object in the MIB tree. Use the following procedure to create or remove a view entry with MIB objects to be included or excluded from user access. The views are associated with each group to restrict or allow access to the OIDs.

### NOTE

View creation is not supported on the Brocade VDX 2746.

1. Enter the **configure** command.
2. Enter the **snmp-server view** *view-name* *mib\_tree* **{included | excluded}** command.

```
switch(config)# snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

Enter the **no** form of the command to remove the configured SNMP server view entry.

The following is an example to create a SNMP view entry "view1" with excluded permission for the MIB object ID "1.3.6.1.2.1.1.3" create a SNMP view entry "view1" with excluded permission for the MIB object ID "1.3.6.1.2.1.1.3":

```
switch(config)# snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

The following is an example to create SNMP view entry "view2" with included permission for the MIB object ID "1.3.6.1":

```
switch(config)# snmp-server view view2 1.3.6.1 included
```

The following is an example to remove the SNMP view entry "view1" from the configuration list:

```
switch(config)# no snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

#### NOTE

The maximum number of views supported with MIB tree entries is 10.

## Configuring SNMP server groups

SNMP groups map the SNMP user for the version v3 and the community for the versions v1 and v2c to SNMP views. Each SNMP group can be configured with a read view with read-only access, a write view with read-write access, and a notify view to trap notifications to be encrypted and sent to target hosts, or all of the above. Users who are mapped to a group with SNMP view can use its views for access control.

The authoring parameter determines the authentication and privacy required by the users to access the view. The auth **auth** | **noauth** | **priv** parameter is available when you select v3, not v1 or v2.

Use the following procedure to configure or remove a specified SNMP group.

#### NOTE

Group creation is not supported for the Brocade VDX 2746. Only the default groups snmpadmin and snmpuser are supported.

1. Enter the **configure** command.
2. Enter the **snmp-server group** *groupname* {v1 | v2c | v3 {auth | noauth | priv}} [read *viewname*] [write *viewname*] [notify *viewname*] command.

```
switch(config)# snmp-server group group1 v3 auth read myview write view1 notify view1
```

Enter the **no** form of the command to remove the configured SNMP server group.

#### NOTE

The maximum number of SNMP groups supported is 10.

The following is an example to create SNMP server group entries for SNMPv3 user group with auth/noauth permission:

```
switch(config)# snmp-server group admin v3 auth read view2 write view2 notify view2
switch(config)# snmp-server group admin1 v3 noauth read view1 write view1 notify view1
```

The following is an example to remove the configured SNMP server groups:

```
switch(config)# no snmp-server group admin v3 auth read view2 write view2
switch(config)# no snmp-server group admin v3 noauth read view1 write view1 notify view1
```

## Configuring SNMP server users

The **snmp-server user** command configures a SNMPv3 user and allows the configured user to be associated with user-defined SNMP groups. You can execute this command in global configuration mode and RBridge ID configuration mode.

1. Enter the **configure** command to access global configuration mode.

```
switch# configure
```

2. Enter the **snmp-server user** command.

The following example configures the SNMPv3 users "user1" and "user2" associated with user-defined group "group1" under global configuration mode.

```
switch(config)# snmp-server user user1 groupname group1
switch(config)# snmp-server user user2 groupname group1 auth md5 auth-password password priv DES
priv-password
```

The following example configures the SNMPv3 users "user1" and "user2" associated with user-defined group "group1" under global configuration mode. It also applies an IPv4 ACL and an IPv6 ACL to "user1."

```
switch(config)# snmp-server user user1 groupname group1 ipv4-acl standV4ACL1 ipv6-acl standV6ACL1
switch(config)# snmp-server user user2 groupname group1 auth md5 auth-password password priv DES
priv-password
```

### NOTE

You can associate only global SNMPv3 users with ACLs. For the entire flow of implementing SNMP ACLs, refer to [Implementation flow of ACLs under SNMP](#) on page 134.

The following example configures the SNMPv3 user "snmpadmin1" under RBridge ID configuration mode.

```
switch(config-rbridge-id-1)# snmp-server user snmpadmin1 groupname snmpadmin auth sha auth-password
private123 priv DES priv-password public123
```

### NOTE

When creating a new SNMPv3 user without the **groupname** option, by default there is no group name mapped with the SNMPv3 user. You must map the configured SNMPv3 user with a group name available in the group CLI configuration to contact the switch through SNMPv3.

### NOTE

The behavior of this command in RBridge ID configuration mode is same as in global configuration mode. If the user name is configured to be the same in both global and RBridge ID configurations, the RBridge ID configuration takes precedence. The encrypted password generated in global configuration mode can be used for another global user to modify the passwords. The encrypted passwords generated in global configurations cannot be used in RBridge ID configurations, and vice versa.

## Configuring password encryption for SNMPv3 users

For SNMPv3 users, the passwords for **auth-password** and **priv-password** are encrypted. You can configure either with a plain-text password or an encrypted password. In both cases, the passwords are shown in the **show running-config** command as encrypted.

The following example shows a plain-text password configuration:

```
switch(config)# snmp-server user snmpadmin1 auth md5 auth-password private123 priv DES priv-password
public123
```

The following example shows an encrypted password configuration:

```
switch(config)# snmp-server user snmpadmin2 groupname snmpadmin auth md5 authpassword "MvB
+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA== \n" encrypted
```

**NOTE**

This command may not be successful where encrypted passwords are generated by third-party or open-source tools.

## Configuring SNMP server v3hosts

The `snmp-server v3host` command configures a SNMPv3 host by associating with the SNMP users. You execute this command in global configuration mode and RBridge ID configuration mode.

Refer to the *Network OS Command Reference* for complete descriptions of all the SNMPv3 server host options.

1. Enter the `configure` command.
2. Enter the `snmp-server v3host` command to associate the users to the host.

```
switch(config)# snmp-server v3host 1050::5:600:300c:326b snmpadmin2 severity-level Info use-vrf
default-vrf
```

This example configures the SNMPv3 trap IPv6 host 1050:0:0:0:5:600:300c:326b associated with SNMP user "snmpadmin2" under global configuration mode with default vrf.

```
switch(config-rbridge-id-1)# snmp-server v3host 10.26.3.166 snmpuser2 severity-level Info udp-port
4425
```

This example configures the SNMPv3 trap host 10.26.3.166 associated with SNMP user "snmpuser2" under RBridge ID configuration mode.

The global SNMPv3 host can be configured by associating with only global SNMPv3 users and the local SNMPv3 host can be configured by associating with only local SNMPv3 users. You cannot create a SNMPv3 host in global configuration by associating with the local SNMPv3 users and vice versa.

The `no snmp-server v3host` command removes the SNMP server v3host from the switch configuration altogether.

## Managing SNMP access rights using ACLs

Access lists (ACLs) enable you to permit or deny SNMP access by IP address.

SNMP server groups enable you to specify read, write, and notify permissions for the following entities:

- Community, under SNMPv1 and SNMPv2c
- User, under SNMPv3

For SNMP packets that pass community/user validation, access lists (ACLs) offer an additional permit/deny level, filtered by IP addresses that you specify.

If SNMP ACLs are applied, the validation order is as follows:

1. SNMP-server validation (community/user string). If not validated, the SNMP packet is dropped.
2. Server-ACL validation
  - If there is a **deny** match—including an explicit or implicit `deny any` rule—the packet is dropped.

**NOTE**

Unless you include an explicit `permit any` rule, an implicit `deny any` rule is automatically applied for IP addresses not explicitly permitted.

- If there is a **permit** match—including a `permit any` rule—validation continues.
3. Server-group validation, the concluding step of the validation flow

## Implementation flow of ACLs under SNMP

The implementation flow for ACLs under SNMP is as follows:

1. Create access lists (ACLs) that permit or deny specified IP addresses. For details, refer to [Creating standard ACLs for SNMP](#) on page 134.
2. Define server groups with the needed combination of Read or Write; and Notify permissions. For details, refer to [Adding an SNMP community string](#) on page 127.
3. For SNMPv1 or SNMPv2c, implement [Adding an SNMP community string](#) on page 127.
4. For SNMPv3, implement [Configuring SNMP server users](#) on page 132.

## Creating standard ACLs for SNMP

Use these procedures to create access lists (ACLs) that contain rules permitting or denying access from specified IP addresses.

### Creating an IPv4 ACL for SNMP

A standard ACL permits or denies traffic according to source address only. SNMP supports only standard ACLs.

1. Enter **configure** to access global configuration mode.

```
switch# configure
```

2. Enter the **ip access-list standard** command to create the access list.

```
switch(config)# ip access-list standard stdACL3
```

3. For each ACL rule, enter a **seq** command, specifying the needed parameters.

```
switch(config-ipacl-std)# seq 5 permit host 10.20.33.4
switch(config-ipacl-std)# seq 15 deny any
```

The following example does the following, under SNMPv3:

1. Creates a IPv4 standard ACL named "test".
2. Defines rules that permits packets from a specified host and denies packets from any other host.
3. Configures the SNMP server user "user1", including application of the "test" IPv4 ACL.

```
switch(config)# ip access-list standard test
switch(conf-ipacl-std)# permit host 10.1.1.1
switch(conf-ipacl-std)# deny any
switch(conf-ipacl-std)# exit
switch(config)# snmp-server user user1 groupname snmpadmin auth sha auth-password private123 priv DES priv-
password public123 ipv4-acl test
```

### Creating an IPv6 ACL for SNMP

A standard ACL permits or denies traffic according to source address only. SNMP supports only standard ACLs.

1. Enter **configure** to access global configuration mode.

```
switch# configure
```

2. Enter the **ipv6 access-list standard** command to create the access list.

```
switch(config)# ipv6 access-list standard std_V6_ACL4
```

- For each ACL rule, enter a **[seq] {permit | deny | hard-drop}** command, specifying the needed parameters.

```
switch(config-ip6acl-std)# seq 5 permit host 2001:db8::1:2
switch(config-ip6acl-std)# seq 15 deny any
```

The following example does the following, under SNMPv1 or SNMPv2c:

- Creates an IPv6 standard ACL named "stdv6acl".
- Defines rules that permits packets from a specified host and denies packets from any other host.
- Configures the SNMP server community "c1", including application of the "stdv6acl" IPv6 ACL.

```
switch(config)# ipv6 access-list standard stdv6acl
switch(conf-ip6acl-std)# permit fe::/24
switch(conf-ip6acl-std)# deny any
switch(conf-ip6acl-std)# exit
switch(config)# snmp-server community c1 groupname admin ipv6-acl stdv6acl
```

## Displaying SNMP configurations

Use the **show running-config snmp-server** command to display the current SNMP configurations for the SNMP host, community string, contact, and location, as well as other SNMP configuration options such as SNMPv3 host address, context, VRF mapping, and applied ACLs.

Enter the **show running-config snmp-server** command.

```
switch# show running-config snmp-server

snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server enable trap
snmp-server community ConvergedNetwork groupname user
snmp-server community OrigEquipMfr groupname admin
snmp-server community "Secret C0de" groupname admin
snmp-server community c1 groupname admin ipv4-acl test ipv6-acl stdv6acl
snmp-server community c2 groupname g1 ipv4-acl 1 ipv6-acl 2
snmp-server community com1
snmp-server community common groupname user
snmp-server community private groupname admin
snmp-server community public groupname user
snmp-server host 10.20.53.161 private
  severity-level Info
  use-vrf mgmt-vrf
!
snmp-server user snmpadmin1 groupname user
snmp-server user snmpadmin2 groupname snmpadmin
snmp-server user snmpadmin3 groupname snmpadmin
snmp-server user snmpuser1 groupname snmpuser
snmp-server user snmpuser2 groupname snmpuser
snmp-server user snmpuser3 groupname snmpuser
snmp-server user user1 groupname admin auth sha auth-password "ggc+pJR30+ORXd6OULEU6GaUFN4=\n" priv DES
priv-password "4qrmMZ5wR1W9MQMKxrQWFpaAgl8=\n" encrypted ipv4-acl test ipv6-acl stdv6acl
snmp-server view All 1 included
snmp-server group admin v1 read All write All notify All
snmp-server group admin v2c read All write All notify All
snmp-server group snmpadmin v3 notify All
snmp-server group snmpuser v3 notify All
snmp-server group user v1 read All notify All
snmp-server group user v2c read All notify All
```

## Enabling and disabling SNMP server trap link-status

The **snmp-server trap-link status** command is available under the following interface sub-modes.

- Physical interface
- Virtual Ethernet (VE) interface
- Port-Channel interface
- Loopback interface

Under all the above interfaces, the traps are enabled by default. Enter the **no snmp-server trap-link status** command to disable the linkUp trap or linkDown trap under an interface. As the traps are enabled by default, the **no** form of the command is not displayed under the **show running-config** command.

## Enabling and disabling the SNMP server offline-if enable

The **no snmp-server offline-if enable** command is used to enable the command behavior to display the interfaces belonging to an offline slot. By default, this behavior is disabled. The new behavior is enabled via SNMP. This command will only change the behavior of SNMP with respect to interfaces on an offline slot. There is no change in the behavior of any existing CLI commands.

When the **no linecard** command is executed on a particular slot, the interfaces related to that slot will not be displayed via SNMP as well, irrespective of whether the offline slot interface display behavior is enabled or disabled. For more information on **no linecard** command, refer to the "linecard" command in the *Network OS Command Reference*.

### NOTE

The **no snmp-server offline-if enable** command only applies to chassis systems and not to pizza box switches.

## Configuring tuple representation for IF-MIB objects

You can configure whether the ifDescr and ifName objects that belong to the Interfaces Group MIB (IF-MIB) are represented in 2-tuple or 3-tuple format.

By default, 2-tuple representation is implemented.

1. From global configuration mode, enter RBridge ID configuration mode.

```
device# configure terminal
device(config)# rbridge-id 1
```

2. Enter the **snmp-server three-tuple-if enable** command.

```
device(config-rbridge-id-1)# snmp-server three-tuple-if enable
```

### NOTE

The results of this command will appear in the running configuration only when it is enabled. The behavior is the same in both logical chassis cluster and fabric cluster modes. Following an upgrade to Network OS 7.0.1, this option is disabled by default, and the ifDescr and ifName objects are represented as 2-tuple.

3. Use the **no** form of this command to return to the default behavior (2-tuple representation).

```
device(config-rbridge-id-1)# no snmp-server three-tuple-if enable
```



# Metro VCS

- Metro VCS overview.....137
- Configuring a long-distance ISL.....145
- Configuring interconnected Ethernet Fabrics.....146
- Using Diagnostic Port for link traffic tests.....148

## Metro VCS overview

Metro VCS allows you to interconnect different locations and form clusters of data centers over long distance in order to provide disaster protection/recovery and load sharing.

### NOTE

Metro VCS is not supported by IP Fabrics.

In cases where distances are moderate, within 30km, and where either dedicated fiber or transparent wavelength services are available, the Metro VCS approach is a good and cost-effective Layer 2 interconnect solution. Due to the multi-pathing capabilities of the TRILL-based Metro VCS solution there is no issue with topology loops between multiple DC locations.

For longer distances alternative solutions are available.

- **Interconnecting separate fabrics through Layer 2 point-to-point connectivity** -- Layer 2 point-to-point connectivity is used to interconnect VCS Fabrics using their Edge-Ports. If more than one Layer 2 link is needed for capacity or for redundancy reasons, link aggregation (LAG/vLAG) can be used in order to avoid loops between the VCS Fabric edge ports and allow for active/active protection.
- **Interconnecting separate fabrics through Layer 2-VPN connectivity** -- VCS Fabrics are interconnected through their edge ports using Layer 2-VPN connectivity. This can be implemented with Layer 2-VPN services from Connectivity Service Providers or using VPLS functionality implemented on Brocade MLX routers.

FIGURE 22 Metro VCS configuration example



Both options are distance independent in relation to the speed of the protocols used (for example, LAG/vLAG is a slow protocol) and provide flat Layer 2 interconnection between multiple locations. In the case of more than two DC locations, care needs to be taken in order to avoid any topology loops.

## Metro VCS details and configuration

Metro VCS allows for interconnection of different locations and allows to form clusters of data centers over metro distances (<10/30 km) in order to provide disaster protection/recovery and application load sharing.

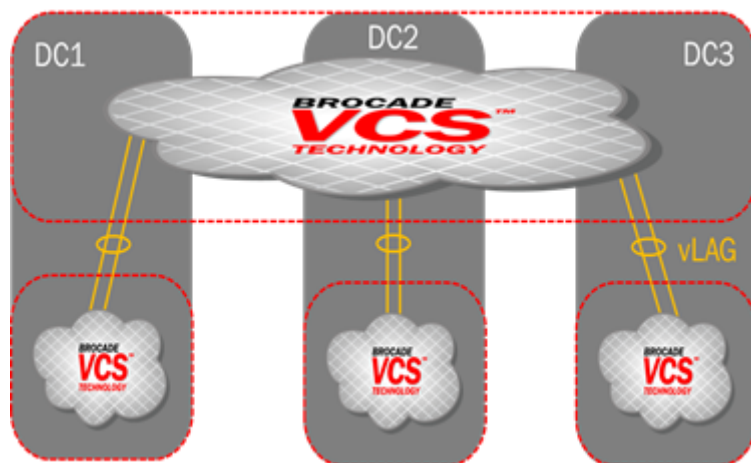
By using Inter-Switch Links (ISLs) over longer distances (more than the standard 1000 m), Ethernet fabrics can be distributed across data centers located in geographically different locations.

FIGURE 23 Basic Metro VCS configuration



If more complex setups are needed within different locations, then local VCS Fabrics can be used interconnected via a stretched interconnect fabrics.

FIGURE 24 Complex Metro VCS configuration



Standard VCS Fabrics scaling limitations apply if Inter-Switch Links (ISLs) are used over distances of up to 1000 m. Using Inter-Switch Links (ISLs) over longer distances (more than the standard 1000 m) is currently available for 10G, 40G, and 100G ISLs and can be done in two ways:

- **Configuring long-distance ISLs (LD-ISLs)** -- This is supported only on 10G ISLs does not restrict fabric topologies (such as the numbers of nodes and number of locations) beyond the standard VCS Fabric scalability. LD-ISLs can be used over distances up to 10km if lossless services (DCB, FCoE) are needed and over distances of 30km if only standard Ethernet is needed.
- **Using standard ISLs over longer distances** -- This only works for restricted topologies (a maximum of 6 nodes and 3 locations) and for standard Ethernet (lossless Ethernet capabilities, such as no FCoE or lossless iSCSI, cannot be used in this case). The

standard 10G ISL can be used over distances up to 30 km, and standard 40G and 100G ISLs can support distances up to 10 km.

## Metro VCS using long-distance ISLs

Extending Ethernet Fabrics over distance is accomplished by using long-distance ISLs. The buffer allocation within a single port group is optimized, which extends the supported ISL distance.

Metro VCS supports long-distance ISL ports up to 30 km on the Brocade VDX platforms listed in the following table. Links up to 10 km are lossless.

**TABLE 23** Limitations for long-distance Metro VCS

Supported hardware	Extended ISL up to 2 km	Extended ISL up to 5 km	Extended ISL up to 10 km	Extended ISL up to 30 km
Brocade VDX 6740	yes	yes	yes	yes
Brocade VDX 6940-144S - 10GbE interface	yes	yes	yes	yes
Brocade VDX 8770 - LC48x10G linecard	yes	yes	yes	yes
Brocade VDX 6940-144S - 10GbE interface	yes	yes	yes	yes

The following table lists the conditions on extended ISLs for Network OS hardware.

**TABLE 24** Conditions for long-distance Metro VCS

Condition	Extended ISL up to 2 km	Extended ISL up to 5 km	Extended ISL up to 10 km	Extended ISL up to 30 km
Support for lossless FCoE/iSCSI traffic on the Metro VCS port group	yes	yes	yes	no
Layer 2/IP lossy traffic support	yes	yes	yes	yes
Number of Metro VCS long-distance ports supported per port group	1	1	1	1
Number of regular ISLs supported on a port group configured for long distance	1	1	0	0
Trunking support between multiple long-distance ISLs	no	no	no	no
CEE map or FCoE port allowed in same port group	no	no	no	no
eNS Sync (MAC address table sync)	yes	yes	yes	yes
Zoning	yes	yes	yes	yes
HA failover	yes	yes	yes	yes
Node redundancy check	yes	yes	yes	yes
vMotion	yes	yes	yes	yes
Maximum PFCs supported	3 (2 on the Brocade VDX 6740)	3(2 on the Brocade VDX 6740)	3 (2 on the Brocade VDX 6740)	3 (2 on the Brocade VDX 6740)

**TABLE 24** Conditions for long-distance Metro VCS (continued)

Condition	Extended ISL up to 2 km	Extended ISL up to 5 km	Extended ISL up to 10 km	Extended ISL up to 30 km
Long-distance ISL on 40G to 4x10G breakout interfaces	no	no	no	no
Long-distance ISL on 1G and 10G copper interfaces	no	no	no	no

The following table lists the port groups and number of port groups available on each platform for long-distance Metro VCS.

**TABLE 25** Long-distance Metro VCS port-group schema

Platform	Port groups	Number of port groups on platform
Brocade VDX 6740	1-32, 33-48 (49-52 are 40G ports and do not support long distance)	2 *
Brocade VDX 6940-144S - 10GbE interface	1-24+61-72, 25-48+73-84, 49-60, 85-96	4
Brocade VDX 8770 (LC48x10G linecard)	1-8, 9-16, 17-24, 25-32, 33-40, 41-48	6 per 10GbE blade
Brocade VDX 6940-144S - 10GbE interface	1-24+61-72, 25-48+73-84, 49-60, 85-96	4

\* Not a valid deployment scenario at distances longer than 5 km, as no normal ISLs are allowed if both port groups are configured with long-distance ISLs for 10 km and 30 km.

## Guidelines and restrictions for long-distance Metro VCS

Consider the following guidelines and restrictions when configuring long-distance Metro VCS:

- Long-distance-ISLs are only supported on 10G interface links.
- Only one long-distance-ISL is supported within a single port group.
- Long-distance-ISL is not supported on 10G copper RJ-45 interfaces
- Long-distance-ISL is not supported on 40G-to-10G breakout interfaces
- Brocade trunking is not supported with long-distance ISLs, but up to eight 8-link ECMP trunks can be used.
- Edge ports within the same port group where a long-distance ISL is configured cannot be configured with DCB maps.
- Edge ports within the same port group where a long-distance ISL is configured cannot be configured by means of the **fcoeport default** command.
- A maximum of three PFCs can be supported on a Metro VCS configured platform. By default, PFC is enabled by class 3 and 7.
- The Brocade VDX 6740 switches support only two PFCs.
- All the ports in the port group are rebooted when a port is configured for long distance.
- For 2-, 5-, 10-km long distance, use Brocade-supported long-range (LR) optics for direct connectivity.
- For 30-km long distance, use Brocade-supported extended-range (ER) optics for direct connectivity.
- A port group containing a long-distance port cannot have a CEE map configuration on any edge port.
- For 2-km and 5-km long-distance ISLs, one additional standard ISL connection is supported on the same long-distance port group.
- Lossless FCoE traffic is supported up to 10 km with long-distance ISL configured.
- Lossy Layer 2/Layer 3 traffic is supported up to 30 km with long-distance ISL configured.

## Metro VCS using standard-distance ISLs

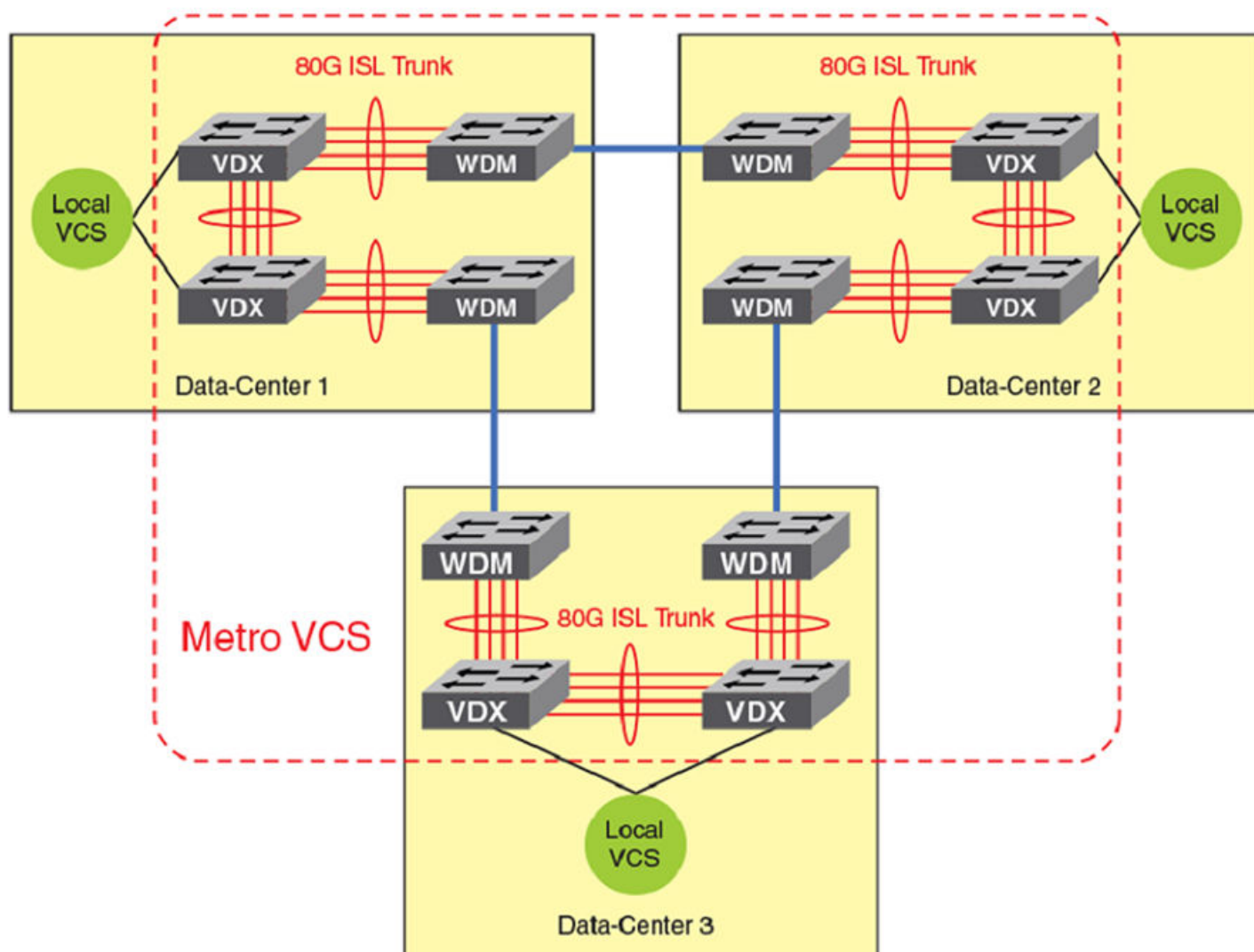
In order to deploy Metro VCS using standard-distance ISLs, no configuration is required on the ISL. The default configuration on the 10-, 40-, and 100-Gbps interface by means of the **fabric isl enable** and **fabric trunk enable** commands allows ISL formation with other Brocade VDX switches in the same VCS cluster automatically. BLDP negotiation takes place to form ISLs for distances up to 80 km for 10G and 40 km for 40G and 100G interfaces. (Refer to the "Configuring Brocade VCS Fabrics" task.)

Metro VCS using standard ISLs is supported on the following platforms:

- Brocade VDX 2741
- Brocade VDX 2746
- Brocade VDX 6740, VDX 6740T, and VDX 6740T-1G
- Brocade VDX 8770 with the LC48X10G line card
- Brocade VDX 8770 with the LC27X40G line card
- Brocade VDX 8770 with the LC12X40G line card
- Brocade VDX 8770 with the LC6X100G line card
- Brocade VDX 6940-36Q
- Brocade VDX 6940-144S

The following figure is an example deployment topology supported for interconnecting data centers by extending Brocade VCS Ethernet fabrics using standard-distance ISLs. The local VCS clusters are connected to the Metro VCS clusters by Brocade vLAGs. In this case, local data-center Ethernet fabrics from both site are not merged while providing seamless Layer 2 extension. For Metro VCS, Brocade standard-distance ISL supports trunks up to a maximum of 80 Gbps for the Brocade VDX 8770 and Brocade VDX 6740 series platforms, or 120 Gbps for Brocade VDX 6940 series platforms.

FIGURE 25 Typical deployment topology for Metro VCS using standard-distance ISLs



The following table lists the port groups and number of port groups available on each platform for Metro VCS using standard-distance ISLs.

TABLE 26 Standard Metro VCS port-group schema

Platform	Port groups	Number of port groups on platform
Brocade VDX 6740	1-16, 17-32, 33-40, 41-48, 49-50, 51-52	6
Brocade VDX 6740T	49-50, 51-52 (40G interfaces only)	2
Brocade VDX 6740T-1G	49-50, 51-52 (40G interfaces only)	2
Brocade VDX 8770 (LC6X100G)	1-2, 3-4, 5-6	3
Brocade VDX 8770 (LC27X40G)	1-3, 4-6, 7-9, 10-12, 13-15, 16-18, 19-21, 22-24, 25-27	9
Brocade VDX 8770 (LC12X40G)	1-2, 3-4, 5-6, 7-8, 9-10, 11-12	6

**TABLE 26** Standard Metro VCS port-group schema (continued)

Platform	Port groups	Number of port groups on platform
Brocade VDX 8770 (LC48x10G line card)	1-8, 9-16, 17-24, 25-32, 33-40, 41-48	6
Brocade VDX 6940-36Q	1-6, 7-12, 13-18, 19-24, 25-30, 31-36	6
Brocade VDX 6940-144S	1-24+61-72, 25-48+73-84, 49-60+97-102, 85-96+1-3-108	4

## Guidelines and restrictions for standard-distance Metro VCS

Consider the following guidelines and restrictions when configuring Metro VCS with standard-distance ISLs:

- Only two data-center and three data-center topologies are supported.
- A maximum of two nodes are supported for each site, which provides node redundancy. If more-complex local designs are required, a local VCS sub-fabric design must be used.
- Only standard Ethernet services are supported, lossless Ethernet capabilities, such as no FCoE or lossless iSCSI, cannot be used in this case.
- Brocade trunking up to 80G (8x10G or 2x40G) or 120G (3x40G or 12x10G):
  - VDX 8770: 8x10G
  - VDX 6740: 8x10G and 2x40G
  - VDX 6740T: 2x40G
  - VDX 6740T-1G: 2x40G
  - VDX 6940-36Q: 3x40G or 12x10G
  - VDX 6940-144S: 3x40G and 12x10G

## Metro VCS combined with vLAGs

Outside of Metro distances, and whenever bit transparency may be a problem, edge-to-edge interconnected fabrics using 10G, 40G, or 100G vLAG over multiple standard Ethernet links can be used. This allows you to connect separate Ethernet fabrics that can be located in different data centers, even if the distance between those locations up to 80 km for 10G interfaces and up to 40 km for 40G and 100G interfaces.

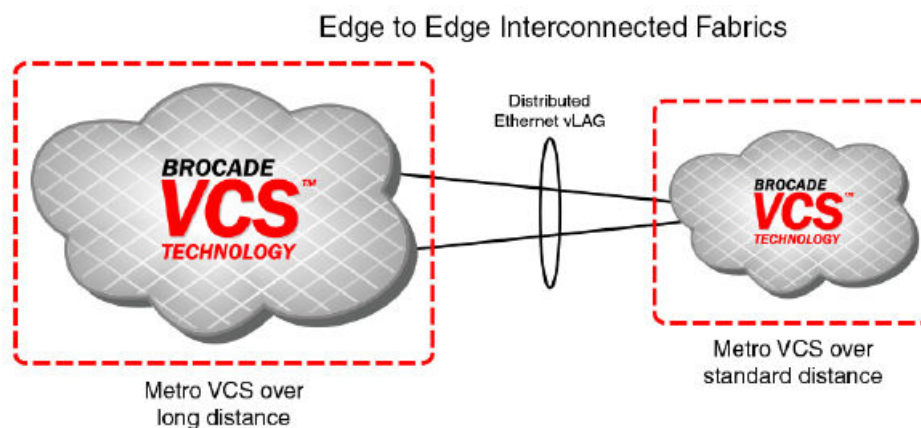
## Metro VCS over a long-distance fabric

Whenever standard VCS Fabrics are interconnected through LAG/vLAG, they are not limited beyond LAG/vLAG protocol capabilities.

Metro VCS Fabrics (stretched fabrics) that are interconnected with standard fabrics are supported for distances up to 100 km.

As shown in the following figure, one side can be a Metro VCS over a long-distance fabric.

FIGURE 26 Metro VCS and distributed Ethernet fabrics



In all deployment with interconnects using edge ports, lossless Ethernet traffic (DCB/FCoE) is not supported.

In order to connect two distinct VCS Ethernet fabrics between data centers, a third Metro VCS fabric can be formed, and the distinct local VCS Ethernet fabrics can connect to the Metro VCS fabric by means of Virtual Link Aggregation (vLAG).

Alternatively, the distinct VCS Ethernet fabrics in the respective data centers can be directly connected to each other by means of vLAG over xWDM up to a distance of 10 or 30 km. Wherever bit-transparency is not achievable in xWDM equipment, this solution can be successfully deployed for edge-to-edge interconnectivity (using 10G, 40G, or 100G vLAGs over multiple standard Ethernet links). This deployment is referred to as "Distributed Ethernet Fabrics using vLAG."

This implementation eliminates the need for the creation of a separate Metro VCS fabric to achieve local VCS cluster isolation while providing Layer 2 connectivity. In such a deployment, DCB/FCoE lossless Ethernet traffic is not supported.

#### NOTE

When a port-channel from a node in one VCS spans across multiple RBridges in other VCS cluster, a vLAG is formed on the RBridges in the VCS cluster that are part of the same port-channel. For Distributed Ethernet Fabrics using vLAG over long distances, only LACP-based standard port-channels are supported. For details on how to create port-channels and vLAGs, refer to "Configuring Link Aggregation" chapter of the *Network OS Layer 2 Switching Configuration Guide*.

### Supported platforms for Distributed Ethernet Fabrics using vLAG

The following VDX platforms are supported for Distributed Ethernet Fabrics using vLAG:

- Brocade VDX 6740, 6740T, and 6740T-1G
- Brocade VDX 8770 with the LC48X10G line card
- Brocade VDX 8770 with the LC27X40G line card
- Brocade VDX 8770 with the LC12X40G line card
- Brocade VDX 8770 with the LC6X100G line card
- Brocade VDX 6940-36Q
- Brocade VDX 6940-144S

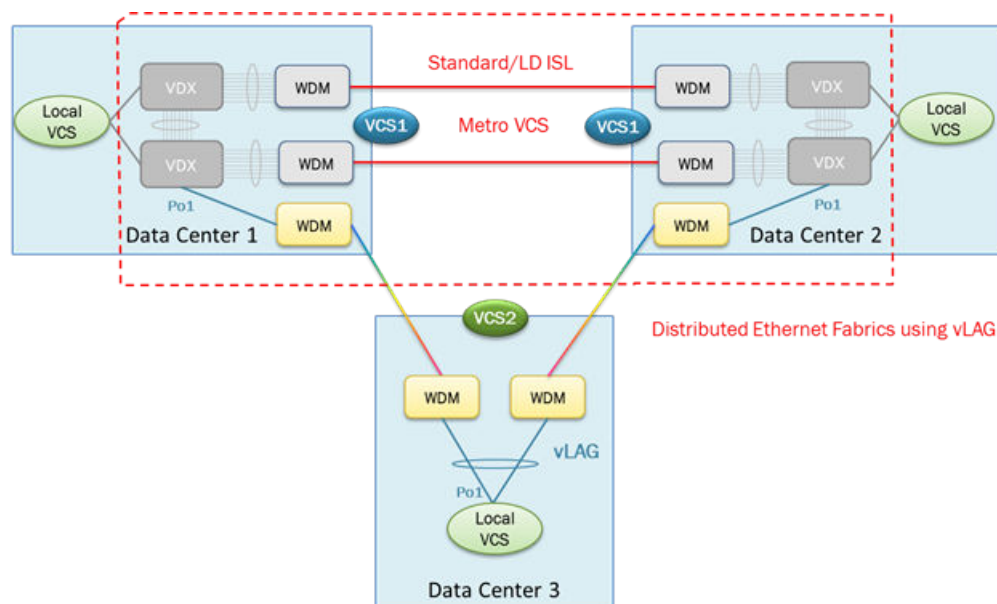


## Topology for Distributed Ethernet Fabrics using vLAG

When a port-channel from a node in one VCS spans across multiple R Bridges in other VCS cluster, a vLAG is formed on the R Bridges in the VCS cluster that are part of the same port-channel. For Distributed Ethernet Fabrics using vLAG over long distances, only LACP-based standard port-channels are supported. For details on how to create port-channels and vLAGs, refer to *Configuring Link Aggregation* in the *Layer 2 Switching Configuration Guide*.

The following figure is a typical deployment topology that uses distributed Ethernet Fabrics using vLAG to interconnect data centers. Nodes from the local VCS cluster are connected by means of xWDM to the nodes in a distant VCS clusters to form a vLAG in between. The distant VCS cluster can be a standard VCS cluster or could be spanned across two data centers over standard-distance or long-distance ISLs, as shown in the figure below. In this case, the vLAG between the two data centers provides VCS fabric isolation while providing seamless Layer 2 connectivity.

**FIGURE 27** Connecting local VCS clusters over long distance using vLAG



## Guidelines and restrictions for Distributed Ethernet Fabrics using vLAG

Note the following guidelines and restrictions for Distributed Ethernet Fabrics using vLAG.

- Only dynamic vLAG is supported.
- DCB/FCoE lossless Ethernet traffic is not supported.
- The maximum distance between standard VCS Fabrics is not limited beyond the capabilities of the LAG/vLAG protocol.
- The maximum supported distance between a stretched Fabric (Metro VCS) and an additional standard VCS Fabric connected through a vLAG is limited to 100 km.

## Configuring a long-distance ISL

To configure a long-distance ISL, perform the following steps in privileged EXEC mode. Each long-distance ISL port of a VCS must be connected to a long-distance ISL port on the remote VCS.

1. Verify that the default standard-distance ISL configuration is correct by using the **show running-config** command.

```
switch# show running-config interface tengigabitethernet 51/0/1
interface TenGigabitEthernet 51/0/1
fabric isl enable
fabric trunk enable
no shutdown
```

2. Set the port to support Metro VCS up to 30 km by using the **long-distance-isl** command.

```
switch# interface tengigabit 51/0/1
switch(conf-if-te-51/0/1)# long-distance-isl 30000
```

3. Perform the same long-distance ISL configuration on the interface of the peer RBridge on the remote sites of the Metro VCS.
4. Verify that the long-distance ISL is correctly formed by using the **show fabric isl** and **show fabric islports** command.

```
switch(conf-if-te-51/0/1)# do show fabric isl
Rbridge-id: 51 #ISLs: 1
  Src      Src      Nbr      Nbr
Index  Interface  Index  Interface  Nbr-WWN      BW  Trunk  Nbr-Name
-----
4      Te 51/0/1    4      Te 53/0/1    10:00:00:05:33:65:3B:50  10G  Yes   "VCS3-53"
switch(conf-if-te-51/0/1)# do show fabric islports
Name:      VCS3-51
Type:      131.4
State:     Online
Role:      Fabric Principal
VCS Id:    3
Config Mode:Local-Only
Rbridge-id: 51
WWN:       10:00:00:05:33:e5:d0:4b
FCF MAC:   00:05:33:e5:d0:cf
  Index  Interface  State  Operational State
  =====
  0      Fo 51/0/49  Down
  1      Fo 51/0/50  Down
  2      Fo 51/0/51  Down
  3      Fo 51/0/52  Down
  4      Te 51/0/1    Up     ISL 10:00:00:05:33:65:3B:50 "VCS3-53" (Trunk Primary)
<Truncated>
```

5. Use the **show ip interface brief** command to confirm the configuration, making sure that Status is "up" and Protocol is "LD ISL," as in the following example output.

```
switch# show ip interface brief

Interface                IP_Address      VRF              Status           Protocol
=====
TenGigabitEthernet 51/0/1  unassigned     default-vrf     up              up (LD ISL)
```

## Configuring interconnected Ethernet Fabrics

To deploy interconnected Ethernet Fabrics using vLAG, create a port-channel interface on the R Bridges that are to be connected. Then add the member interfaces to the port-channel and bring them online. Configure switchport and add the VLANs that are to be allowed over the port-channel. After the port-channels on all the R Bridges are online, the vLAG forms automatically on the R Bridge that connects to multiple nodes on the other VCS cluster. In the deployment topology shown in [Topology for Distributed Ethernet Fabrics using vLAG](#) on page 145, the vLAG forms on the R Bridges that are part of port-channel Po1 in Data-Centers 1 and 2 that forms VCS 1.

This configuration must be applied on R Bridges that connect the two VCS instances. Perform the following task in global configuration mode.

1. Create a port-channel interface on all R Bridges that are directly connected to R Bridges in other VCS instances.

**NOTE**

In logical chassis cluster mode, the port-channel is created only from the principal node and is applied globally.

```
switch(config)# interface port-channel 300
```

2. Verify that the port-channel is created correctly by using the **show running-config** command.

```
switch(config-Port-channel-300)# do show running-config interface port-channel 300

interface Port-channel 300
 vlag ignore-split
 shutdown
```

3. Configure the port-channel interface for the switchport trunk and add the VLANs to be allowed on the trunk interface by using the **switchport** command.

```
switch(config-Port-channel-300)# switchport
switch(config-Port-channel-300)# switchport mode trunk
switch(config-Port-channel-300)# switchport trunk allowed vlan all
```

4. Verify the port-channel interface configuration by using the **show running-config** command.

```
switch(config-Port-channel-300)# do show running-config interface Port-channel 300

interface Port-channel 300
 vlag ignore-split
 switchport
 switchport mode trunk
 switchport trunk allowed vlan all
 switchport trunk tag native-vlan
 spanning-tree shutdown
 shutdown
```

5. Add member interfaces to the port-channel interface by using the **channel-group** command. Do this for all interfaces that must be part of the port-channel.

```
switch(conf-if-te-53/0/31)# channel-group 300 mode active type standard
switch(conf-if-te-53/0/31)# do show running-config interface

TenGigabitEthernet 53/0/31
interface TenGigabitEthernet 53/0/31
 fabric isl enable
 fabric trunk enable
 channel-group 300 mode active type standard
 lacp timeout long
 no shutdown
```

6. Bring the port-channel online in both VCS instances by executing **no shutdown** on the port-channel interface.

```
switch(config-Port-channel-300)# no shutdown
```

7. Verify the port-channel interface configuration by using the **show running-config** command.

```
switch(config-Port-channel-300)# do show running-config interface Port-channel 300

interface Port-channel 300
 vlag ignore-split
 switchport
 switchport mode trunk
 switchport trunk allowed vlan all
 switchport trunk tag native-vlan
 spanning-tree shutdown
 no shutdown
```

8. Verify that console RASLogs indicate the formation of the vLAG by using the **no shutdown** command.

```
switch(config-Port-channel-300)# no shutdown

2013/06/17-16:40:53, [NSM-1023], 224126, DCE, INFO, VCS1-51, RBridge ID 51 has joined Port-channel
300. Port-channel is a vLAG with RBridge IDs 52 51.
```

9. Verify the formation of the port-channel vLAG by using the **show port-channel** command.

```
switch# show port-channel 300
LACP Aggregator: Po 300 (vLAG)
Aggregator type: Standard
Ignore-split is enabled
Member rbridges:
  rbridge-id: 51 (2)
  rbridge-id: 52 (2)
Admin Key: 0010 - Oper Key 0010
Partner System ID - 0x8000,01-e0-52-00-00-02
Partner Oper Key 0010
Member ports on rbridge-id 51:
  Link: Te 51/0/31 (0x19180E801C) sync: 1
  Link: Te 51/0/32 (0x19180F001D) sync: 1
```

## Using Diagnostic Port for link traffic tests

The Diagnostic Port (D\_Port) feature allows you to convert a TRILL ISL port into a diagnostic port for testing link traffic between a pair of switches. The test results can be very useful in diagnosing a variety of port and link problems.

For details, see the "Diagnostic Port" chapter in the *Network OS Administration Guide*.

# Zones

---

- [Zoning overview](#).....149
- [Configuring and managing zones](#) .....156

## Zoning overview

Zoning is a fabric-based service that enables you to partition your network into logical groups of devices that can access each other and prevent access from outside the group. Grouping devices into zones in this manner not only provides security, but also relieves the network from Registered State Change Notification (RSCN) storms that occur when too many native FCoE devices attempt to communicate with one another.

You can use zoning to partition your network in many ways. For example, you can partition your network into two zones, *winzone* and *unixzone*, so that your Windows servers and storage do not interact with your UNIX servers and storage. You can use zones to logically consolidate equipment for efficiency or to facilitate time-sensitive functions; for example, you can create a temporary zone to back up nonmember devices.

A device in a zone can communicate only with other devices connected to the fabric within the same zone. A device not included in the zone is not available to members of that zone. When zoning is enabled, devices that are not included in *any* zone configuration are inaccessible to all other devices in the fabric.

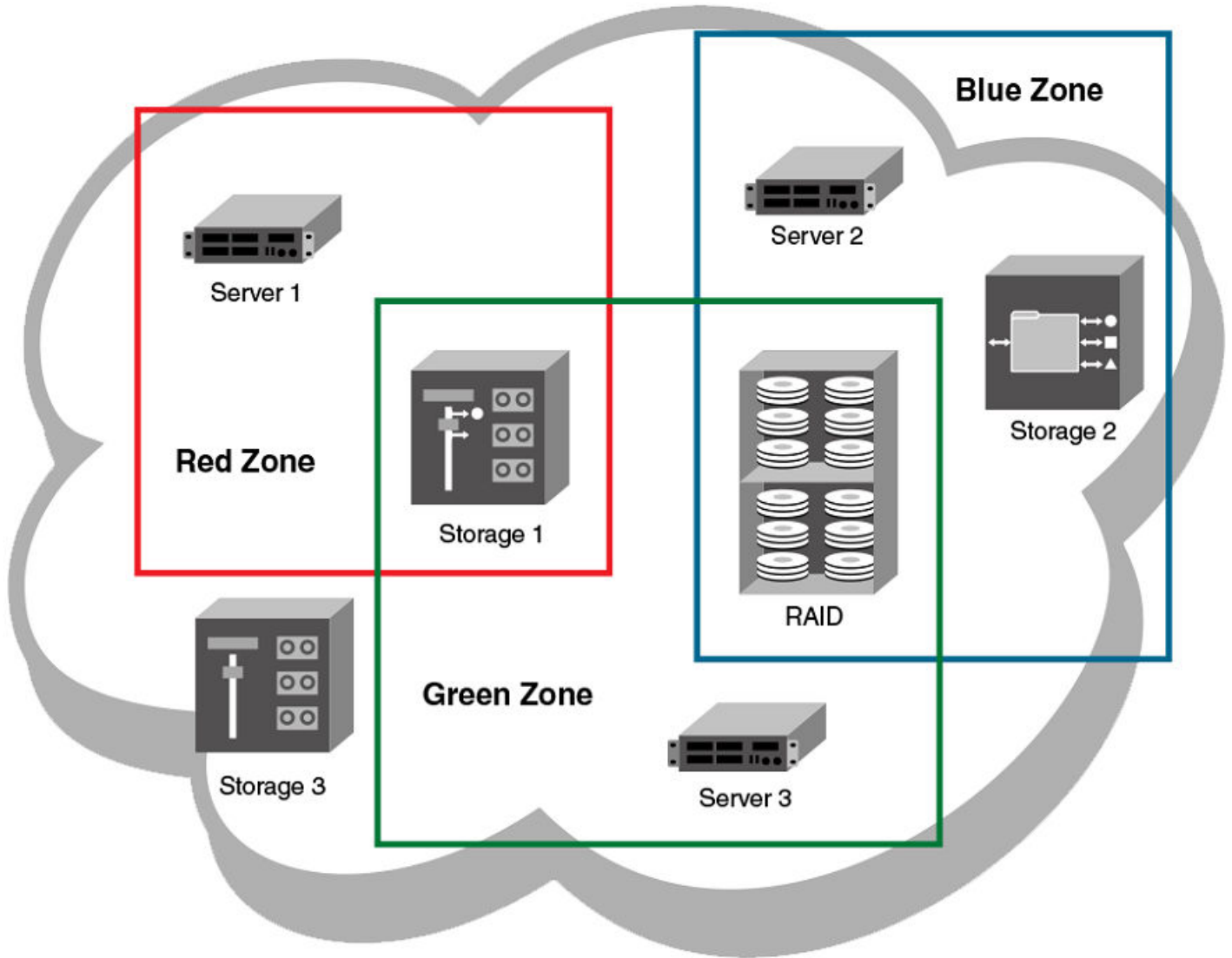
Zones can be configured dynamically. They can vary in size, depending on the number of fabric-connected devices, and devices can belong to more than one zone.

## Example zoning topology

Consider the following figure, which shows three configured zones: Red, Green, and Blue. In this figure the following is true:

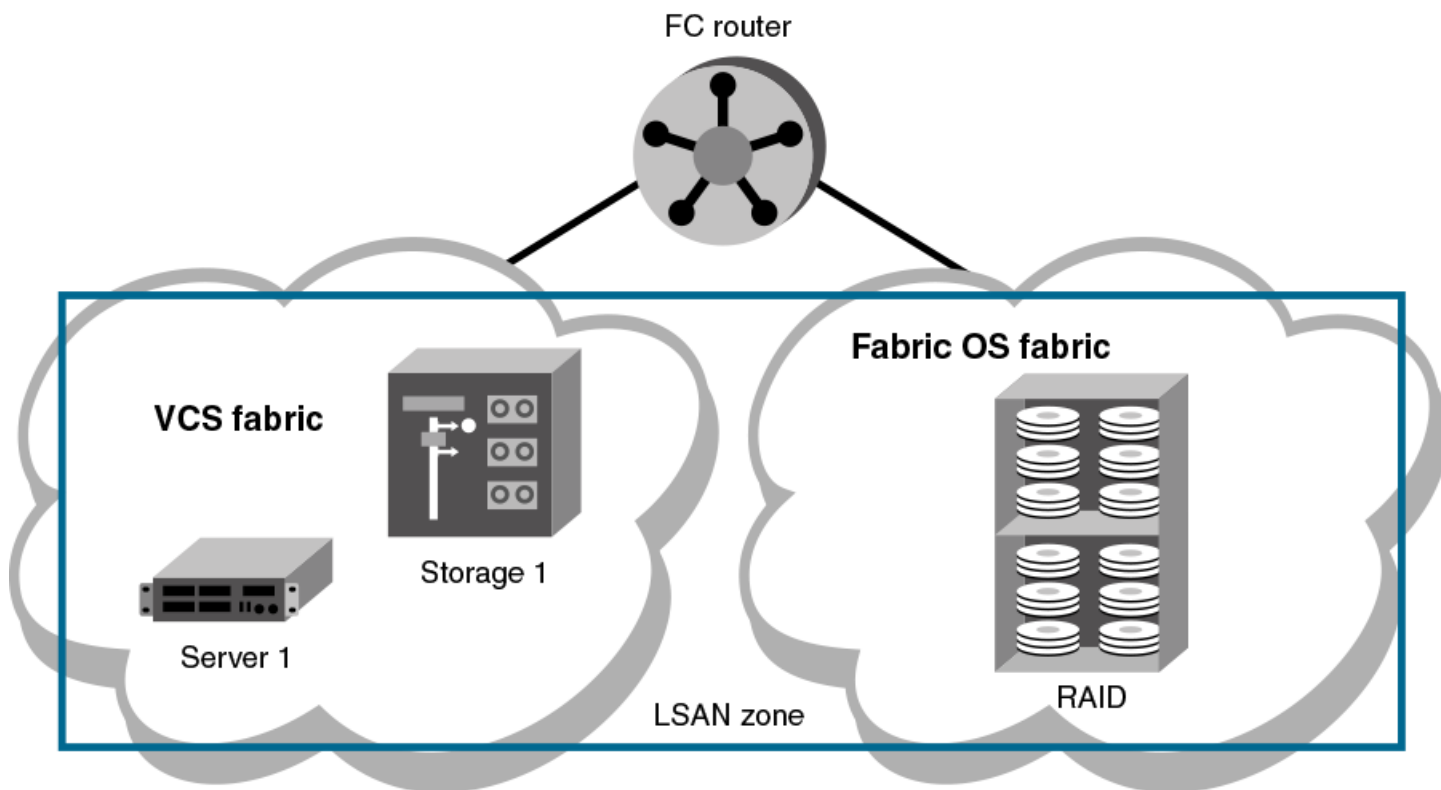
- Server 1 can communicate only with the Storage 1 device.
- Server 2 can communicate only with the RAID and Storage 2 devices.
- Server 3 can communicate with the RAID and Storage 1 devices.
- The Storage 3 is not assigned to a zone; no other zoned fabric device can access it.

FIGURE 28 Zoning



Connecting to another network through a Fibre Channel (FC) router, you can create a Logical SAN (LSAN) zone to include zone objects on other fabrics, including Fabric OS networks. No merging takes place across the FC router when you create an LSAN zone. The figure below shows an example in which Server 1, which is connected to switch in a Brocade VCS Fabric cluster, has access to local storage and to RAID storage on a Fabric OS fabric. (For a detailed discussion of LSAN zones, refer to [LSAN zones](#) on page 151.)

FIGURE 29 LSAN zoning

**NOTE**

Zoning in Network OS 4.0.0 and later has the following restrictions:

- Zone objects based on physical port number or port ID (D,I ports) are not supported.
- You cannot access a target on a Network OS fabric from a server on the Fabric OS fabric.

## LSAN zones

LSAN zones are distinct from conventional zones. This section details how to define and manage LSAN zones and provides recommendations about LSAN zone naming.

### LSAN zones overview

A Logical SAN (LSAN) consists of zones in two or more edge or backbone fabrics that contain the same devices. LSANs essentially provide selective device connectivity between fabrics without forcing you to merge those fabrics. FC routers provide multiple mechanisms to manage inter-fabric device connectivity through extensions to existing switch management interfaces. For details of this FC-FC routing service, refer to the *Fabric OS Administrator's Guide*.

**NOTE**

A backbone fabric consists of one or more FC switches with configured EX\_Ports. These EX\_Ports in the backbone connect to edge fabric switches through E\_Ports. This type of EX\_Port-to-E\_Port connectivity is called an "*Inter-Fabric Link (IFL)*".

The Brocade VCS Fabric connection to the FC router is an ISL that connects an FC port on a Brocade VDX 6740 to an EX\_Port on the FC router. Similarly, an FC port on the Fabric OS fabric connects to an EX\_Port on the FC router.

You can define and manage LSANs using the same zone management tools as for regular zones. The FC router makes LSAN zoning possible by importing devices in effective zones. For example, consider two devices:

- 11:22:33:44:55:66:77:99 is connected to a switch in a Brocade VCS Fabric cluster.
- 11:22:33:44:55:66:77:88 is connected to a switch in a Fabric OS fabric.

The FC-FC routing service on the FC router that connects the two fabrics presents 11:22:33:44:55:66:77:88 as a phantom device to the Brocade VCS Fabric and also presents 11:22:33:44:55:66:77:99 as a phantom device to the Fabric OS fabric. You can then use the regular zone management tools on the Brocade VCS Fabric cluster to incorporate 11:22:33:44:55:66:77:99 into an LSAN zone on the Brocade VCS Fabric. Similarly, you can use the regular zone management tools in Fabric OS to incorporate 11:22:33:44:55:66:77:88 into an LSAN zone in the Fabric OS fabric. Once both the Brocade VCS Fabric zone and the Fabric OS zone are enabled, the FC router imports devices common to both zones and makes them available to the zones in each fabric.

## LSAN naming

Zones that contain hosts and targets that are shared between the two fabrics need to be explicitly coordinated. To share devices between any two fabrics, you must create an LSAN zone in both fabrics containing the WWNs of the devices to be shared. Although you manage an LSAN zone by using the same tools as any other zone on the edge fabric, two behaviors distinguish an LSAN zone from a conventional zone:

- A required naming convention. The name of an LSAN zone begins with the prefix "LSAN\_". The LSAN name is case-insensitive; for example, `lsan_` is equivalent to `LSAN_`, `Lsan_`, and so on.
- LSAN zone members in all fabrics must be identified by their WWN. You cannot use the port IDs that are supported only in Fabric OS fabrics.

### NOTE

The "LSAN\_" prefix must appear at the beginning of the zone name.

To enable device sharing across multiple fabrics, you must create LSAN zones on the edge fabrics (and optionally on the backbone fabric as well), using normal zoning operations to create zones with names that begin with the special prefix "LSAN\_", and adding host and target port WWNs from both local and remote fabrics to each local zone as desired. Zones on the backbone and on multiple edge fabrics that share a common set of devices will be recognized as constituting a single multi-fabric LSAN zone, and the devices that they have in common will be able to communicate with each other across fabric boundaries.

## Managing domain IDs

FCoE connectivity across the Fibre Channel link between Brocade VCS Fabric clusters and FC routers uses domain IDs to identify switches. Within a Brocade VCS Fabric cluster, a domain ID is the same as a routing bridge ID. When you connect to a Fibre Channel router, the FC Fabric Fibre Channel router service emulates virtual *phantom* FC domains in the FCoE fabric. Each FCR-enabled switch emulates a single "front" phantom domain and each FC fabric is represented by a *translate* phantom domain.

It is important to ensure that front domain IDs and translate domain IDs presented by the FC router do not overlap routing bridge IDs in the FCoE fabric; otherwise, the connectivity will fail and the Network OS switch with the overlapping routing bridge ID becomes isolated from the fabric. To prevent potential overlap, use the `portCfgExport -d` Fabric OS command on the FC router to apply a unique front domain ID — one that will not be used in the FCoE fabric. Similarly, use the `fcrXlateConfig importedFID exportedFID preferredDomainID` Fabric OS command to set the translate domain ID to a unique value that is also not used as a routing bridge ID.

Refer to the *Fabric OS Command Reference Manual* for details about the `portCfgExport` and `fcrXlateConfig` commands.



## Approaches to zoning

The following table lists the various approaches you can take when implementing zoning in a Network OS fabric.

**TABLE 27** Approaches to fabric-based zoning

Zoning approach	Description
<b>Recommended approach</b>	
Single HBA	Zoning by single HBA most closely re-creates the original SCSI bus. Each zone created has only one HBA (initiator) in the zone; each of the target devices is added to the zone. Typically, a zone is created for the HBA and the disk storage ports are added. If the HBA also accesses tape devices, a second zone is created with the HBA and associated tape devices in it. In the case of clustered systems, it could be appropriate to have an HBA from each of the cluster members included in the zone; this zoning is equivalent to having a shared SCSI bus between the cluster members and assumes that the clustering software can manage access to the shared devices.  In a large fabric, zoning by single HBA requires the creation of possibly hundreds of zones; however, each zone contains only a few members. Zone changes affect the smallest possible number of devices, minimizing the impact of an incorrect zone change. <i>This zoning philosophy is the preferred method.</i>
<b>Alternative approaches</b>	
Application	Zoning by application typically requires zoning multiple, perhaps incompatible, operating systems into the same zones. This method of zoning creates the possibility that a minor server in the application suite could disrupt a major server (such as a Web server disrupting a data warehouse server). Zoning by application can also result in a zone with a large number of members, meaning that more notifications, such as RSCNs, or errors, go out to a larger group than necessary.
Operating system	Zoning by operating system has issues similar to zoning by application. In a large site, this type of zone can become very large and complex. When zone changes are made, they typically involve applications rather than a particular server type. If members of different operating system clusters can detect storage assigned to another cluster, they might attempt to own the other cluster's storage and compromise the stability of the clusters.
Port allocation	Avoid zoning by port allocation unless the administration team has very rigidly enforced processes for port and device allocation in the fabric. It does, however, provide some positive features. For instance, when a storage port, server HBA, or tape drive is replaced, the change of WWN for the new device is of no consequence. As long as the new device is connected to the original port, it continues to have the same access rights. The ports on the edge switches can be pre-associated to storage ports, and control of the fan-in ratio (the ratio of the input port to output port) can be established. With this pre-assigning technique, the administrative team cannot overload any one storage port by associating too many servers with it.
<b>Not recommended</b>	
No zoning	Using no zoning is the least desirable zoning option because it allows devices to have unrestricted access on the fabric and causes RSCN storms. Additionally, any device attached to the fabric, intentionally or maliciously, likewise has unrestricted access to the fabric. This form of zoning should be used only in a small and tightly controlled environment, such as when host-based zoning or LUN masking is deployed.

## Zone objects

A zone object can be one of the following types: a zone, a zone member, an alias for one or more zone members, or a zoning configuration.

## Zones

A zone is made up of one or more zone members. Each zone member can be a device, a port, or an alias. If the zone member is a device, it must be identified by its Node World Wide Name (node WWN). If it is a port, it must be identified by its Port World Wide Name (port WWN). Port WWNs and node WWNs can be mixed in the same zone. For LSAN zones, only port WWNs can be used.

World Wide Names are specified as 8-byte (16-digit) hexadecimal numbers, separated by colons (:) for example, 10:00:00:90:69:00:00:8a. When a zone object is the node WWN, only the specified device is in the zone. When a zone object is the port WWN name, only the single port is in the zone.

**NOTE**

You are not restricted from configuring more than 255 zone members. However, that figure is considered a best-practices limit, and exceeding it can lead to unpredictable results leading to the possibility of a severe failure condition.

## Zone aliases

A zone alias is a name assigned to a device or a group of devices. By creating an alias, you can assign a familiar name to one or more devices and refer to these devices by that name. Aliases simplify cumbersome data entry by allowing you to create an intuitive naming structure (such as using "NT\_Hosts" to define all NT hosts in the fabric).

As a shortcut for zone members, zone aliases simplify the entry and tracking of zone objects that are defined by their WWNs. For example, you can use the name "Eng" as an alias for "10:00:00:80:33:3f:aa:11".

Naming zones for the initiator they contain can also be useful. For example, if you use the alias SRV\_MAILSERVER\_SLT5 to designate a mail server in PCI slot 5, then the alias for the associated zone is ZNE\_MAILSERVER\_SLT5. This kind of naming strategy clearly identifies the server host bus adapter (HBA associated with the zone).

## Zone configurations

A *zone configuration* is a group of one or more zones. A zone can be included in more than one zone configuration. When a zone configuration is enabled, all zones that are members of that configuration are enabled.

Several zone configurations can reside on a switch at once, and you can quickly alternate between them. For example, you might want to have one configuration enabled during the business hours and another enabled overnight. However, only one zone configuration can be enabled at a time.

The different types of zone configurations are:

- Defined Configuration

The complete set of all zone objects defined in the fabric.

- Enabled Configuration

A single zone configuration that is currently in effect. The enabled configuration is built when you enable a specified zone configuration.

If you disable the enabled configuration, zoning is disabled on the fabric, and default zoning takes effect. When default zoning takes effect, either all devices within the fabric can communicate with all other devices, or no device communicate with any other device, depending on how default zoning is configured. Disabling the configuration does not mean that the zone database is deleted, however, only that no configuration is active in the fabric.

On power-up, the switch automatically reloads the saved configuration. If a configuration was active when it was saved, the same configuration is reinstated on the local switch.

## Naming conventions

Naming zones and zone configurations is flexible. You can devise prefixes to differentiate between zones used for production, backup, recovery, or testing. One configuration should be named PROD\_*fabricname*, where *fabricname* is the name that the fabric has been assigned. The purpose of the PROD configuration is to easily identify the configuration that can be implemented and provide the most generic services. If you want to use other configurations for specific purposes, you can use names such as "BACKUP\_A," "RECOVERY\_2," and "TEST\_18jun02".

## Zoning enforcement

Zone enforcement is by name server. The name server filters queries and RSCNs based on the enabled zoning configuration.

## Considerations for zoning architecture

This table lists considerations for zoning architecture.

**TABLE 28** Considerations for zoning architecture

Item	Description
Effect of changes in a production fabric	Zone changes in a production fabric can result in a disruption of I/O under conditions when an RSCN is issued because of the zone change and the HBA is unable to process the RSCN fast enough. Although RSCNs are a normal part of a functioning SAN, the pause in I/O might not be acceptable. For these reasons, you should perform zone changes only when the resulting behavior is predictable and acceptable. Ensuring that the HBA drivers are current can shorten the response time in relation to the RSCN.
Allowing time to propagate changes	Zoning commands make changes that affect the entire fabric. When executing fabric-level configuration tasks, allow time for the changes to propagate across the fabric before executing any subsequent commands. For a large fabric, you should wait several minutes between commands.
Confirming operation	After changing or enabling a zone configuration, you should confirm that the nodes and storage can identify and access one another. Depending on the platform, you might need to reboot one or more nodes in the fabric with the new changes.
Use of aliases	The use of aliases is optional with zoning. Using aliases requires structure when defining zones. Aliases aid administrators of zoned fabrics in understanding the structure and context of zoning.

## Operational considerations for zoning

Consider the following topics when configuring zoning.

### Zoning configuration changes

When you save, enable, or disable a configuration, the changes are automatically distributed to all switches in the VCS Fabric.

### Supported firmware for zoning

Zoning is supported only if all R Bridges in the fabric are running Network OS 2.1 or later.

Connecting an R Bridge running Network OS 2.0 to an R Bridge running Network OS 2.1 or later merges the two networks only if the R Bridge running Network OS 2.1 or later is in Brocade VCS Fabric mode and no zone database elements are defined or enabled.

A switch running Network OS v3.0.0 will segment if it is attached to a switch running Network OS v2.0.0 regardless of zoning configuration. A switch running Network OS v3.0.0 will join the fabric with a 2.1.x switch and zones will be merged, but the cluster will not form, so no further zoning commands will be allowed until all switches are upgraded to the same firmware version and the cluster has formed.

The Inter-Switch Links (ISLs) connecting the two R Bridges will segment if the R Bridge running Network OS 2.1 or later has any zone defined or enabled, or the default zone is set to No Access. Any such configuration requires automatic distribution of zoning configuration data, which is not compatible with R Bridges running Network OS 2.0.

### Firmware downgrade and upgrade considerations for zoning

A firmware downgrade from Network OS 4.1.0 to Network OS 2.1.x is not permitted under the following conditions:

1. One or more zone aliases are configured on the switch. You must remove all references to zone aliases prior to a firmware downgrade. Use the **no zoning defined-configuration alias** command to delete all zone alias objects. Then issue the **zoning enabled-configuration cfg-action{cfg-save | cfg-disable}** command or the **zoning enabled-configuration cfg-name *cfg\_name*** command to commit the operation before re-attempting a firmware download.
2. An open zone transaction in progress. You must either commit or abort the current open transaction before re-attempting a firmware download. Use the **zoning enabled-configuration cfg-action {cfg-save | cfg-disable}** command or the **zoning enabled-**

**configuration cfg-name cfg\_name** command to commit the current open transaction. Alternately, use the **zoning enabled-configuration cfg-action cfg-transaction-abort** command to abort the open transaction.

You cannot downgrade any switch in a Brocade VCS Fabric to Network OS 2.0 or earlier if any zone definition exists in the defined configuration. Any attempt to do so will fail while attempting to download the earlier firmware. For the downgrade to succeed, you must clear the defined configuration, disable any active configuration, set the default zoning mode to *All Access*, and then try again to download the firmware.

When you upgrade from Network OS 2.1.0 to versions 2.1.1 or later, the zone database is cleared.



#### CAUTION

Clearing the defined configuration clears the zoning database for the entire fabric. If you want to downgrade just one switch without affecting the rest of the fabric, disconnect the switch from the fabric before deleting the defined configuration.

## Configuring and managing zones

### Zone configuration management overview

You can perform zoning operations on any RBridge in the VCS Fabric, but they are always executed on the principal RBridge. In Logical Chassis mode, any edits made to the zoning database are allowed only from the principal RBridge, and you can issue **show** commands from non-principal switches in this mode. In Fabric Cluster mode, you can make edits from any RBridge.

Automatic distribution of the zoning configuration ensures that the effects of these operations are shared and instantly visible on all switches in the VCS Fabric. However, these operations are not permanent until a transaction commit operation saves them to nonvolatile memory, which holds the master copy of the zoning database. In fabric cluster mode, any user can commit the transaction on any switch, and the commit operation saves the operations performed by all users. Once the zoning configuration is saved in permanent memory, it persists across reboot operations.

A transaction commit occurs when you or another user initiates any of the following zoning operations:

- Saving the database to nonvolatile memory with the **zoning enabled-configuration cfg-action cfg-save** command.
- Enable a specific zone configuration with the **zoning enabled-configuration cfg-name** command.
- Disabling the currently enabled zone configuration with the **no zoning enabled-configuration cfg-name** command.

Executing the **zoning enabled-configuration cfg-action cfg-transaction-abort** command cancels the currently open transaction.

If the principal RBridge reboots or goes down, Network OS selects a new principal and any pending zoning transaction is rolled back to the last committed transaction, which is the effective zoning configuration saved in nonvolatile memory. Any changes made to the effective configuration prior to an abort operation must be re-entered.

If an RBridge other than the principal reboots or goes down, the ongoing transaction is not backed out. Any zoning operations initiated by the RBridge are still part of the global transaction maintained on the principal RBridge.

If a fabric segments, the newly elected principal RBridge determines whether transaction data are retained. If a segment retains the original principal, it also retains ongoing transaction data. If a segment elects a new principal, the transaction is aborted.

The zone startup configuration is always equal to the running configuration. The running configuration will always be overwritten by the information from the master copy of the zoning database in nonvolatile memory at startup, so you always start up with the previous running configuration. It is not necessary to copy the running configuration to the startup configuration explicitly.

You can save a snapshot of the current running configuration using the **copy running-config file** command. You can add configuration entries from a saved configuration using the **copy file running-config** command. When saving the snapshot you must ensure that the

saved running configuration contains no zoning transaction data, otherwise failures will occur when you attempt to restore configuration entries from the saved file. Any transaction data would cause such a failure, including empty configuration definitions or empty zones.

## Notes

- When you re-enable the enabled-configuration (using the **zoning enabled-configuration** command) on the principal switch in the cluster, the system propagates the enabled-configuration across the cluster. There is a slight risk of doing this in that the defined-configuration may contain configuration edits that you may not want to enable yet. This feature prevents switches in the cluster from having mismatched enabled-configurations.
- When restoring the running configuration, Brocade recommends copying the file to the running configuration in the absence of any other command line input.
- When you restore a configuration using the **copy** command, the contents of the file are added to the defined configuration; they do not replace the defined configuration. The result is cumulative, is as if the input came from the command line.

## Understanding and managing default zoning access modes

The default zoning mode controls device access if zoning is not implemented or if there is no enabled zone configuration. Default zoning has two access modes:

- *All Access* — All devices within the fabric can communicate with all other devices.
- *No Access* — Devices in the fabric cannot access any other device in the fabric.

The default setting is All Access. Changing the default access mode requires committing the ongoing transaction for the change to take effect.

The default zoning mode takes effect when you disable the effective zone configuration. If your default zone has a large number of devices, to prevent RSCN storms from overloading those devices, you should set the default zoning mode to No Access before attempting to disable the zone configuration. If your default zone includes more than 300 devices, the zoning software prevents you from disabling the zoning configuration if the default zoning mode is All Access.

## Setting the default zoning mode

1. In privileged EXEC mode, enter the **configure terminal** command to enter the global configuration mode.
2. Enter one of the following commands, depending on the default access mode you want to configure:
  - To set the default access mode to All Access, enter **zoning enabled-configuration default-zone-access allaccess**.
  - To set the default access mode to No Access, enter **zoning enabled-configuration default-zone-access noaccess**.
3. Enter the **zoning enabled-configuration cfg-action cfg-save** or **zoning enabled-configuration cfg-name** command to commit the ongoing transaction and save the access mode change to nonvolatile memory.
4. Enter the **show running-config zoning enabled-configuration** command to verify the access mode change.

Example of setting the default zoning mode to no access:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning enabled-configuration default-zone-access noaccess
switch(config)# zoning enabled-configuration cfg-action cfg-save
switch(config)# do show running-config zoning enabled-configuration
zoning enabled-configuration cfg-name cfg1
zoning enabled-configuration default-zone-access noaccess
zoning enabled-configuration cfg-action cfg-save
```

## Understanding and managing zone database size

The maximum size of a zone database is the upper limit for the defined configuration, and it is determined by the amount of memory available for storing the master copy of the defined configuration in flash memory.

Use the following information displayed by the **show zoning operation-info** command to determine whether there is enough space to complete outstanding transactions:

- db-max — Theoretical maximum size of the zoning database kept in nonvolatile memory
- db-avail — Theoretical amount of free space available
- db-committed — The size of the defined configuration currently stored in nonvolatile memory
- db-transaction — The amount of memory required to commit the current transaction

The supported maximum zone database size is 100 KB. If the outstanding transaction data (db-transaction field) is less than the remaining supported space (100 KB minus db-committed), enough space exists to commit the transaction.

### NOTE

The db-max field has a theoretical zone database limit of approximately 1 MB. However, performance might become unacceptable if the zoning database exceeds 150 KB.

## Viewing database size information

In privileged EXEC mode, enter the **show zoning operation-info** command.

Database and transaction size information is displayed in bytes.

```
switch# show zoning operation-info
db-max 1045274
db-avail 1043895
db-committed 367
db-transaction 373
transaction-token 1
last-zone-changed-timestamp 2011-11-16 16:54:31 GMT-7:00
last-zone-committed-timestamp 2011-11-16 16:23:44 GMT-7:00
```

## Managing zone aliases

A zone alias is user-defined name for a logical group of ports or WWNs. You can simplify the process of creating and managing zones by first specifying aliases for zone members. Aliases facilitate tracking and eliminate the need for long lists of individual zone member names. An alias can be a member of a zone, but it cannot be a member of a zoning configuration.

### Creating an alias

1. In privileged EXEC mode, enter the **show name-server detail** command to list the WWNs of devices and targets available in the Brocade VCS Fabric.
2. Enter the **configure terminal** command to enter global configuration mode.
3. Enter the **zoning defined-configuration alias** command followed by a name for the alias.

A subconfiguration mode prompt appears.

4. Enter the subconfiguration mode **member-entry** command to specify at least one member entry.

The member entry must be specified as a port WWN or a node WWN.

You can add multiple members in one operation by separating each member entry with a semicolon (;). No spaces are allowed after the semicolon.

5. Enter the **exit** command to return to global configuration mode.

6. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the configuration to nonvolatile memory.

The following is an example of creating an alias with one member node WWN:

```
switch# show name-server detail
PID: 013100
Port Name: 20:00:00:00:00:00:01
Node Name: 10:00:00:00:00:00:01
(output truncated)
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# member-entry 10:00:00:00:00:00:01
switch(config-alias-alias1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

### Adding additional members to an existing alias

1. In privileged EXEC mode, enter the **show name-server detail** command to list the WWNs of devices and targets available in the Brocade VCS Fabric.
2. Enter the **configure terminal** command to enter global configuration mode.
3. Enter the **zoning defined-configuration alias** command followed the name of an existing zone alias.

A subconfiguration mode prompt appears.

4. Enter the subconfiguration mode **member-entry** command to specify at least one member entry.

The member entry must be specified as a port WWN or a node WWN.

You can add multiple members in one operation by separating each member entry with a semicolon (;). No spaces are allowed after the semicolon.

5. Enter the **exit** command to return to global configuration mode.
6. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the configuration to nonvolatile memory.

Example of adding two member node WWNs to an existing alias:

```
switch# show name-server detail
PID: 013200
Port Name: 20:00:00:00:00:00:02
Node Name: 10:00:00:00:00:00:02
(output truncated)
PID: 013300
Port Name: 20:00:00:00:00:00:03
Node Name: 10:00:00:00:00:00:03
(output truncated)
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# member-entry 10:00:00:00:00:00:02;10:00:00:00:00:00:03
switch(config-alias-alias1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
switch(config)#
```

### Removing a member from an alias

1. In privileged EXEC mode, enter the **show running-config zoning** command to display the alias and its member WWNs.
2. Enter the **configure terminal** command to enter global configuration mode.
3. Enter the **zoning defined-configuration alias** command followed the name of an existing zone alias.

A subconfiguration mode prompt appears.

4. Enter the subconfiguration mode **no member-entry** command to specify the WWN to be removed from the zone alias.  
You can only remove one member at a time.
5. Enter the **exit** command to return to the global configuration mode.
6. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the configuration to nonvolatile memory.

The following provides an example of removing two members from an alias:

```
switch# show running-config zoning
zoning defined-configuration alias alias1
  member-entry 10:00:00:00:00:00:01
  member-entry 10:00:00:00:00:00:02
  member-entry 10:00:00:00:00:00:03
  (output truncated)
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration alias alias1
switch(config-alias-alias1)# no member-entry 10:00:00:00:00:00:02
switch(config-alias-alias1)# no member-entry 10:00:00:00:00:00:03
switch(config-alias-alias1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

## Deleting an alias

1. In privileged EXEC mode, enter the **show running-config zoning** command to display the alias and its member WWNs.
2. Enter the **configure terminal** command to enter global configuration mode.
3. Enter the **no zoning defined-configuration alias** command followed by the name of the alias you want to delete.
4. Enter the **show running-config zoning** command to verify the change in the defined configuration (optional).
5. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the configuration to nonvolatile memory.

Example of deleting an alias:

```
switch# show running-config zoning
zoning defined-configuration alias alias1
  member-entry 10:00:00:00:00:00:01
  !
zoning enabled-configuration cfg-name ""
zoning enabled-configuration default-zone-access allaccess
zoning enabled-configuration cfg-action cfg-none
switch#
switch# configure terminal
Entering configuration mode terminal
switch(config)# no zoning defined-configuration alias alias1
switch(config)# do show running-config zoning
zoning enabled-configuration cfg-name ""
zoning enabled-configuration default-zone-access allaccess
zoning enabled-configuration cfg-action cfg-none
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

## Creating zones

Consider the following topics when creating zones.

### Creating a zone

A zone cannot persist without any zone members. When you create a new zone, the **zoning defined-configuration zone** command places you in a command subconfiguration mode where you can add the first zone member entry. You can specify multiple members by separating each member from the next by a semicolon (;).



**NOTE**

Zones without any zone members cannot exist in volatile memory. They are deleted when the transaction commits successfully.

The following procedure adds a new zone to the defined configuration.

1. In privileged EXEC mode, enter the **show name-server detail** command to obtain the WWNs of servers and targets available in the Brocade VCS Fabric.
2. Enter the **configure terminal** command to enter global configuration mode.
3. Enter the **zoning defined-configuration zone** command and enter a new zone name to add a new zone.  
A subconfiguration mode prompt appears.
4. Enter the subconfiguration mode **member-entry** command to specify at least one member entry.  
The member entry must be specified as a port WWN, a node WWN, or an alias. You can mix WWNs and aliases.  
Add multiple members in one operation by separating each member entry with a semicolon (;). No spaces are allowed after the semicolon.
5. Enter the **exit** command to return to global configuration mode.
6. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the modified configuration to nonvolatile memory.

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

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

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

## Adding a member to a zone

1. In privileged EXEC mode, enter the **show name-server detail** command to list the WWNs of devices and targets available on the Brocade VCS Fabric cluster.
2. Enter the **configure terminal** command to enter global configuration mode.
3. Enter the **zoning defined-configuration zone** command and enter the name of an existing zone.  
A subconfiguration mode prompt appears.
4. Enter the subconfiguration mode **member-entry** command and specify the member you want to add.  
The new member can be specified by a port WWN, a node WWN, or a zone alias.  
Add multiple members in one operation by separating each member with a semicolon (;).
5. Enter the **exit** command to return to the global configuration mode.
6. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the modified configuration to nonvolatile memory.

Example of adding three members to a zone, two node WWNs and an alias:

```
switch# show name-server detail
PID: 012100
Port Name: 50:05:07:61:00:1b:62:ed
Node Name: 50:05:07:61:00:1b:62:ed
(output truncated)
PID: 012200
Port Name: 50:05:07:61:00:09:20:b4
Node Name: 50:05:07:61:00:09:20:b4
(output truncated)

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

## Removing a member from a zone

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **zoning defined-configuration zone** command and enter the name of the zone from which you want to remove a member.

A subconfiguration mode prompt appears.

3. Enter the subconfiguration mode **no member-entry** parameter and specify the WWN or the alias of the member you want to remove.

You can remove only one member at a time. To remove more than one member, you must issue the **no member-entry** command for each member you want to remove.

4. Enter the **exit** command to return to global configuration mode.
5. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the modified configuration to nonvolatile memory.

### NOTE

The parent configuration is removed when the last child object is removed, irrespective of the save operation.

Example of removing more than one member from a zone:

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

## Deleting a zone

Before deleting a zone, ensure that the zone is not a member of any enabled zone configuration. Although the deletion will proceed in RAM, you will not be able to save the configuration to nonvolatile memory if an enabled zone configuration has the deleted zone as a member.

1. In privileged EXEC mode, enter the **show running-config zoning defined-configuration** command and verify that the zone you want to delete is not a member of an enabled zone configuration. If the zone is a member of an enabled zone configuration, remove it.

2. Enter the **configure terminal** command to enter the global configuration mode.
3. Enter the **no zoning defined-configuration zone** command and enter the name of the zone you want to delete.
4. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the modified configuration to nonvolatile memory.

#### NOTE

The parent configuration is removed when the last child object is removed, irrespective of the save operation.

Example of removing a zone from the defined configuration:

```
switch# show running-config zoning defined-configuration
zoning defined-configuration zone zone1
member-entry 10:00:00:00:00:00:01
!
zoning defined-configuration zone zone2
member-entry 10:00:00:00:00:00:02
!
switch# configure terminal
Entering configuration mode terminal
switch(config)# no zoning defined-configuration zone zone2
switch(config)# zoning enabled-configuration cfg-action cfg-save
Updating flash ...
switch(config)# exit
switch# show running-config zoning defined-configuration
zoning defined-configuration zone zone1
member-entry 10:00:00:00:00:00:01
```

## Managing zones

Consider the following topics when managing zones.

### Viewing the defined configuration

To view the defined configuration, in privileged EXEC mode enter the **show running-config zoning defined-configuration** command.

For each configuration, the command lists each member zone. For each zone, the command lists the WWN or alias name of each member. The following example illustrates this.

```
switch# show running-config zoning defined-configuration

zoning defined-configuration cfg cfg0
member-zone zone_0_1
member-zone zone_0_2
member-zone zone_0_3
member-zone zone_0_4
member-zone zone_same
!
zoning defined-configuration cfg cfg1
member-zone zone_1_1
member-zone zone_1_2
member-zone zone_1_3
member-zone zone_1_4
member-zone zone_same
!
zoning defined-configuration cfg cfg2
member-zone zone_2_1
member-zone zone_2_2
member-zone zone_2_3
member-zone zone_2_4
member-zone zone_same
!
zoning defined-configuration cfg cfg4
member-zone zone2
```

```

member-zone zone3
!
zoning defined-configuration zone zone0
member-entry 11:22:33:44:55:66:77:80
member-entry 11:22:33:44:55:66:77:81
member-entry 11:22:33:44:55:66:77:82
member-entry 11:22:33:44:55:66:77:83
member-entry 11:22:33:44:55:66:77:84
!
zoning defined-configuration zone zone1
member-entry 11:22:33:44:55:66:77:80
member-entry 11:22:33:44:55:66:77:81
member-entry 11:22:33:44:55:66:77:82
member-entry 11:22:33:44:55:66:77:83
member-entry 11:22:33:44:55:66:77:84
!
zoning defined-configuration zone zone2
member-entry 11:22:33:44:55:66:77:80
member-entry 11:22:33:44:55:66:77:81
member-entry 11:22:33:44:55:66:77:82
member-entry 11:22:33:44:55:66:77:83
member-entry 11:22:33:44:55:66:77:84
!
      (output truncated)

```

## Viewing the enabled configuration

To view the enabled configuration, in privileged EXEC mode enter the **show zoning enabled-configuration** command. The following information about the enabled configuration is displayed:

- The name of the configuration
- The configuration action
- The mode of the default zone — the mode that will be active if you disable the enabled configuration

### NOTE

In Network OS 4.0.0 and later, the enabled-zone output is no longer available from the **show running-config zoning enabled-configuration enabled-zone** command. It is now available from the **show running-config zoning enabled-configuration** command.

The configuration name has CFG\_MARKER asterisk (\*) appended to it if an outstanding transaction exists; the asterisk is not present if no outstanding transaction exists. Similarly, the configuration action is flagged as "cfg-save" if no outstanding transaction exists; "cfg-none" indicates that an outstanding transaction exists. A CFG\_MARKER flag is appended to the configuration if the enabled configuration does not exactly match the defined configuration. This scenario occurs when you have an enabled configuration and make changes to the defined-configuration, and then, instead of enabling the defined configuration, you issue the **cfg-save** command.



### CAUTION

When edits are made to the defined configuration, and those edits affect a currently enabled zone configuration, issuing a "cfg-save" command makes the enabled configuration effectively stale. Until the enabled configuration is reenabled, the merging of new RBridges into the cluster is not recommended. This merging may cause unpredictable results, with the potential for mismatched enabled-zoning configurations among the RBridges in the cluster.

Example of viewing the zoning enabled configuration:

```

switch# show zoning enabled-configuration

zoning enabled-configuration cfg-name cfg1
zoning enabled-configuration enabled-zone zone1 member-entry 10:00:00:00:00:00:01
zoning enabled-configuration enabled-zone zone2 member-entry 10:00:00:00:00:00:02

```

## Creating a zone configuration

A zone configuration cannot persist without any member zones. When creating a new zone configuration, the **zoning defined-configuration cfg** command places you in a command sub-configuration mode where you must add at least one member zone. While zone configurations without any member zones can exist in volatile memory, they are deleted when the transaction commits successfully.

The following procedure adds a new zone configuration to the defined configuration.

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **zoning defined-configuration cfg** command and enter a new configuration name.  
A subconfiguration mode prompt appears.
3. Enter the **member-zone** subconfiguration mode command and specify the name of at least one zone.  
Add multiple zones in one operation by separating each zone name with a semicolon (;).
4. Enter the **exit** command to return to global configuration mode.
5. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the modified configuration to nonvolatile memory.

Example of creating a zone configuration with one member zone:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration cfg config1
switch(config-cfg-config1)# member-zone zone1
switch(config-cfg-config1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

### NOTE

Zone aliases are not valid zone configuration members. Adding an alias to an existing zone configuration will not be blocked. However, the attempt to enable a zone configuration that contains aliases will fail with an appropriate error message.

## Adding a zone to a zone configuration

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **zoning defined-configuration cfg** command and enter the name of the configuration to which you want to add zones.  
The command prompt changes to indicate a subconfiguration mode.
3. Enter the **member-zone** subconfiguration mode command and specify the name of at least one member zone.  
Add multiple zones in one operation by separating each zone name with a semicolon (;).
4. Enter the **exit** command to return to global configuration mode.
5. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the modified configuration to nonvolatile memory.

Example of adding two zones to config1:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration cfg config1
switch(config-cfg-config1)# member-zone zone2;zone3
switch(config-cfg-config1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

## Removing a zone from a zone configuration

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **zoning defined-configuration cfg** command and enter the name of the configuration from which you want to remove a zone.

The command prompt changes to indicate a subconfiguration mode.

3. Enter the **no member-zone** subconfiguration mode command and specify the name of the zone you want to remove from the configuration.

You can remove only one member at a time. To remove more than one member, you must issue the **no member-zone** command for each member you want to remove.

4. Enter the **exit** command to return to global configuration mode.
5. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the modified configuration to nonvolatile memory.

### NOTE

The parent configuration is removed when the last child object is removed, irrespective of the save operation.

Example of removing two zones from config1:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration cfg config1
switch(config-cfg-config1)# no member-zone zone2
switch(config-cfg-config1)# no member-zone zone3
switch(config-cfg-config1)# exit
switch(config)# zoning enabled-configuration cfg-action cfg-save
```

## Enabling a zone configuration

Only one zone configuration can be enabled in a VCS Fabric. The following procedure selects a configuration from the defined configuration and makes it the enabled configuration. If a zone configuration is currently enabled, the newly enabled configuration replaces the previously enabled configuration.

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **zoning enabled-configuration cfg-name** command with the name of the configuration you want to enable.

In addition to enabling the specified configuration, this command also saves any changes made to the zoning database in volatile memory to nonvolatile memory. The saved configuration is persistent.

If the configuration refers to a nonexistent zone or a zone with no members assigned to it, the operation fails and the command returns an error message. The following example enables config1.

Example of enabling a zone configuration:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning enabled-configuration cfg-name config1
```

Example of a failed enable operation:

The enable operation fails because the configuration contains a zone without members.

```
switch(config)# do show running-config zoning
zoning defined-configuration cfg cfg1
member-zone-zone1
member-zone zone2
!
zoning defined-configuration zone zone1 <-----Zone with no member
```

```

!
zoning defined-configuration zone zone2
member-entry 20:03:00:11:0d:bc:76:09
!
zoning enabled-configuration cfg-name ""
zoning enabled-configuration default-zone-access allaccess
zoning enabled-configuration cfg-action cfg-none
switch(config)# zoning enabled-configuration cfg-name cfg1
% Error: Command Failed. Cfg contains empty zone object "zone1"

```

## Disabling a zone configuration

Disabling the currently enabled configuration returns the fabric to no-zoning mode. All devices can then access one another or not at all, depending on the default zone access mode setting.

### NOTE

For fabrics with many devices, Brocade recommends setting the default zone access mode to No Access before disabling a zone configuration to avoid RSCN storms.

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **no zoning enabled-configuration cfg-name** command.

In addition to disabling the currently enabled configuration, this command also saves any changes made to the zoning database in volatile memory to nonvolatile memory. The saved configuration is persistent.

Example of disabling a zone configuration:

```

switch# configure terminal
Entering configuration mode terminal
switch(config)# no zoning enabled-configuration cfg-name

```

## Deleting a zone configuration

The following procedure deletes a zone configuration from the defined configuration.

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **no zoning defined-configuration cfg** command and the name of the zone configuration you want to delete.
3. Enter the **zoning enabled-configuration cfg-action cfg-save** command to save the modified defined configuration to nonvolatile memory.

Example of deleting a zone configuration:

```

switch# configure terminal
Entering configuration mode terminal
switch(config)# no zoning defined-configuration cfg cfg2
switch(config)# zoning enabled-configuration cfg-action cfg-save

```

### NOTE

If you try to delete the enabled configuration from the defined configuration, the **zoning enabled-configuration cfg-action cfg-save** command returns an error. However, if you commit the transaction with the **zoning enabled-configuration cfg-action cfg-disable** command, the operation proceeds without error.

## Clearing changes to a zone configuration

The following procedure aborts all pending transactions and removes all uncommitted operations from the database. It returns the configuration in volatile memory to the state it was in when a **zoning enabled-configuration cfg-action cfg-save** or **zoning enabled-configuration cfg-name** command was last executed successfully.

1. In privileged EXEC mode, enter the **configure terminal** command to enter the global configuration mode.
2. Enter the **zoning enabled-configuration cfg-action cfg-transaction-abort** command.

Example of aborting a transaction:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning enabled-configuration cfg-action cfg-transaction-abort
```

## Clearing all zone configurations

The following procedure clears all zone configurations from the defined configuration and enables the default zone.

### NOTE

For fabrics with many devices, Brocade recommends setting the default access mode to No Access before clearing all zone configurations to avoid RSCN storms.

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **zoning enabled-configuration cfg-action cfg-clear** command.
3. Enter one of the following commands, depending on whether an enabled zone configuration exists:
  - If no enabled zone configuration exists, enter the **zoning enabled-configuration cfg-action cfg-save** command.
  - If an enabled zone configuration exists, enter the **no zoning enabled-configuration cfg-name** command to disable and clear the zone configuration in nonvolatile memory for all switches in the fabric.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning enabled-configuration cfg-action cfg-clear
switch(config)# no zoning enabled-configuration cfg-name
```

## Backing up the zone configuration

To back up your zoning configuration you copy it to a file and store it on a server or on an attached USB device. You can use the copy to restore the configuration if needed.

### NOTE

Ensure that no transaction is pending before you perform the copy operation, otherwise failures will occur when you attempt to restore configuration entries from the saved file. Any transaction data would cause such a failure, including empty configuration definitions or empty zones.

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Empty the transaction buffer by either committing the transaction to nonvolatile memory or aborting the transaction.
  - To commit the transaction, enter the **zoning enabled-configuration cfg-action cfg-save** command, the **zoning enabled configuration cfg-name** command, or the **zoning enabled-configuration cfg-action cfg-disable** command.
  - To abort the transaction, enter the **zoning enabled-configuration cfg-action cfg-transaction-abort** command.
3. Enter the **exit** command to return to privileged EXEC mode.
4. Enter the **copy** command. For the source file, use **running-config**. For the destination file, use the file name you want the configuration copied to.

Example of making a backup copy on a USB device:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning enabled-configuration cfg-action cfg-save
```



```
switch(config)# exit
switch# copy running-config usb://myconfig
```

## Restoring a configuration from backup

When you restore a configuration from backup and add to the running configuration, the zone configuration identified in the backup copy as the enabled configuration becomes the new enabled configuration.

In privileged EXEC mode, enter the **copy** command. For the source file use the file where the saved configuration is stored. For the destination file, use **running-config**.

This operation updates the defined configuration in RAM.

### NOTE

The **copy** command adds to the defined configuration. It does not replace the defined configuration.

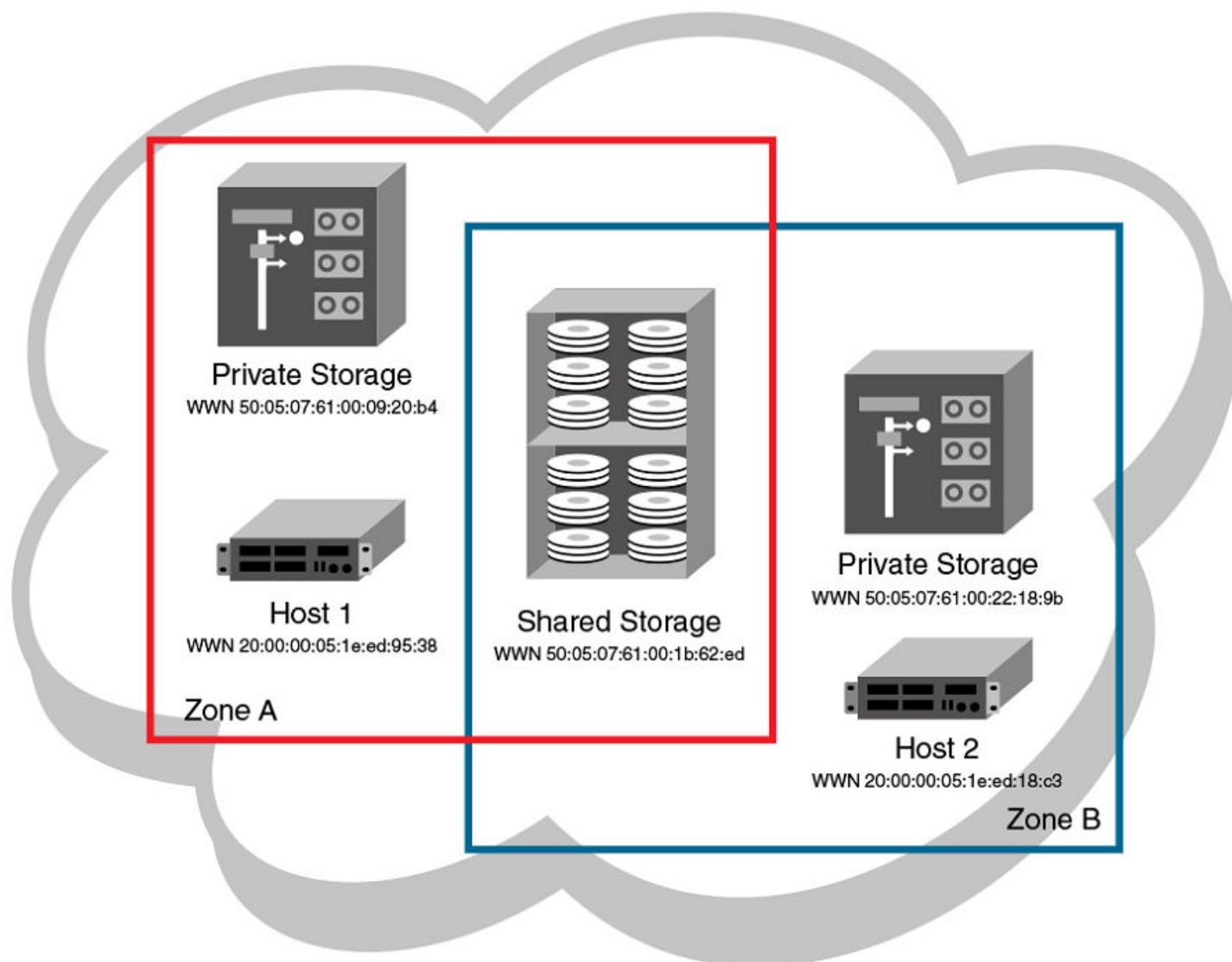
The following example adds the configuration in the file named myconfig on the attached USB device to the defined configuration.

```
switch# copy usb://myconfig running-config
```

## Zone configuration scenario example

This example creates the zone configuration shown below. The example assumes that two hosts need access to the same storage device, while each host needs private storage of its own. You create two zones: Zone A contains Host 1, its private storage device, and the shared storage device; Zone B contains Host 2, its private storage device, and the shared storage device. In addition, you create two zone configurations: cfg1 in which only Zone A is effective; cfg2, in which both zones are effective.

FIGURE 30 Zone configuration example



1. Log in to any switch in the Brocade VCS Fabric.
2. Enter the **show name-server detail** command to list the available WWNs.
3. Enter the **configure terminal** command to enter global configuration mode.
4. Enter the **zoning defined-configuration zone** command to create Zone A.
5. Enter the **zoning defined-configuration zone** command to create Zone B.
6. Enter the **zoning defined-configuration cfg** command to create the configuration `cfg1` with Zone A as its only member.
7. Enter the **zoning defined-configuration cfg** command to create the configuration `cfg2` with Zone A and Zone B as its members.
8. Enter the **zoning running-config defined-configuration** command to view the defined zone configuration.
9. Enter the **zoning enabled-configuration cfg-name** command to enable `cfg2`.

10. Verify the enabled zoning configuration, by means of the **show zoning enabled-configuration** command.

```
switch# show name-server detail
switch# configure terminal
Entering configuration mode terminal
switch(config)# zoning defined-configuration zone ZoneA
switch(config-zone-ZoneA)# member-entry 20:00:00:05:1e:ed:
95:38;50:05:07:61:00:09:20:b4;50:05:07:61:00:1b:62:ed
switch(config-zone-ZoneA)# exit
switch(config)# zoning defined-configuration zone ZoneB
switch(config-zone-ZoneB)# member-entry 20:00:00:05:1e:ed:18:c3;50:05:07:61:00:22:18:9b;
50:05:07:61:00:1b:62:ed
switch(config-zone-ZoneB)# exit
switch(config)# zoning defined-configuration cfg cfg1
switch(config-cfg-cfg1)# member-zone ZoneA
switch(config-cfg-cfg1)# exit
switch(config)# zoning defined-configuration cfg cfg2
switch(config-cfg-cfg2)# member-zone ZoneA;ZoneB
switch(config-cfg-cfg2)# exit
switch(config)# zoning enabled-configuration cfg-name cfg2
switch(config)# exit
switch# show zoning enabled-configuration
zoning enabled-configuration cfg cfg1
  member-zone ZoneA
  !
zoning enabled-configuration cfg cfg2
  member-zone ZoneA
  member-zone ZoneB
  !
zoning enabled-configuration zone ZoneA
  member-entry 20:00:00:05:1e:ed:95:38
  member-entry 50:05:07:61:00:09:20:b4
  member-entry 50:05:07:61:00:1b:62:ed
  !
zoning enabled-configuration zone ZoneB
  member-entry 20:00:00:05:1e:ed:18:c3
  member-entry 50:05:07:61:00:22:18:9b
  member-entry 50:05:07:61:00:1b:62:ed
```

## Merging zones

This section provides the background needed to merge zones successfully. The tables at the end of this section summarize scenarios involving Switch A and Switch B and the results to be expected following a merge.

### Preconditions for zone merging

When a new switch is added to a VCS fabric, it automatically inherits the zone configuration information from the fabric. You can verify the zone configuration on any switch by using the procedure described in [Viewing the defined configuration](#) on page 163. Take care to avoid mismatched enabled-configuration scenarios.



#### CAUTION

When edits are made to the defined configuration, and those edits affect a currently enabled zone configuration, issuing a "cfg-save" command makes the enabled configuration effectively stale. Until the enabled configuration is reenabled, the merging of new R Bridges into the cluster is not recommended. This merging may cause unpredictable results, with the potential for mismatched enabled-zoning configurations among the R Bridges in the cluster.

If you are adding a switch that is already configured for zoning, you must clear the zone configuration on that switch before connecting it to the zoned fabric. Refer to [Clearing all zone configurations](#) on page 168 for instructions.

Adding a new fabric that has no zone configuration information to an existing zoned fabric is very similar to adding a new switch. All switches in the new fabric inherit the zone configuration data. If the existing fabric has an effective zone configuration, then the same configuration becomes the effective configuration for all switches in the added fabric.

#### NOTE

To prevent an unwanted zone merge, use the **no fabric isl enable** command on ISL interfaces instead of the **shutdown** command on tengigabitethernet ports.

Before the new fabric can merge successfully, it must satisfy the following criteria:

- Before merging
  - Ensure that all switches adhere to the default zone merge rules as described in [Zone merging scenarios](#) on page 173.
  - Ensure that the enabled and defined zone configurations match. If they do not match and you merge with another switch, the merge might be successful, but unpredictable zoning and routing behavior can occur. Refer to the Caution in this section and refer to [Viewing the defined configuration](#) on page 163.
- Merging and segmentation

The system checks each port as it comes online to determine whether the ports should be segmented. E\_Ports come online on power up, enabling a switch, or adding a new switch, and the system checks the zone database to detect if the two database that can be merged safely. Refer to [Zone merging scenarios](#) on page 173.

Observe the following rules when merging zones:

- Merging rules
  - Local and adjacent configurations: If the local and adjacent zone database configurations are the same, they will remain unchanged after the merge.
  - Enabled configurations: If there is an enabled configuration between two switches, the enabled zone configurations must match.
  - Zone membership: If a zoning object has the same name in both the local and adjacent defined configurations, the content and order of the members are important.
  - Objects in adjacent configurations: If a zoning object appears in an adjacent defined configuration, but not in the local defined configuration, the zoning object is added to the local defined configuration. The modified zone database must fit in the nonvolatile memory area allotted for the zone database.
  - Local configuration modification: If a local defined configuration is modified because of a merge, the new zone database is propagated to the other switches within the merge request.
- Merging two fabrics

For best practices, the default-zone access modes should match, although this is not a requirement. Refer to [Zone merging scenarios](#) on page 173.

If the two fabrics have conflicting zone configurations, they will not merge. If the two fabrics cannot join, the ISLs between the switches will segment.

The transaction state after the merge depends on which switch is elected as the principal RBridge. The newly elected principal RBridge retains the same transaction information it had before the merge. Transaction data is discarded from any switch that lost its principal status during the merge.

- Merge conflicts

When a merge conflict is present, a merge does not take place and the ISLs will segment.

If the fabrics have different zone configuration data, the system attempts to merge the two sets of zone configuration data. If the zones cannot merge, the ISLs will be segmented.

- A merge is not possible under any of the following conditions:

- Configuration mismatch: Zoning is enabled in both fabrics and the zone configurations that are enabled are different in each fabric.
- Zone Database Size: The zone database size exceeds the maximum limit of another switch.

#### NOTE

If the zone members on two switches are not listed in the same order, the configuration is considered a mismatch, and the switches will segment from the fabric. For example: `cfg1 = z1; z2` is different from `cfg1 = z2; z1`, even though the members of the configuration are the same. If zone members on two switches have the same names defined in the configuration, make sure the zone members are listed in the same order.

## Fabric segmentation and zoning

If the connections between two fabrics are no longer available, the fabric segments into two separate fabrics. Each new fabric retains the previous zone configuration.

If the connections between two fabrics are replaced and no changes have been made to the zone configuration in either of the two fabrics, the two fabrics can merge back into one single fabric. If any changes that cause a conflict have been made to either zone configuration, a fabric merge may fail.

## Zone merging scenarios

The following tables provide information on merging zones and the expected results.

**TABLE 29** Zone merging scenarios: Defined and enabled configurations

Description	Switch A	Switch B	Expected results
<b>Switch A</b> has a defined configuration. <b>Switch B</b> does not have a defined configuration.	defined:cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: none	defined: none  enabled: none	Configuration from <b>Switch A</b> propagates throughout the fabric in an inactive state, because the configuration is not enabled.
<b>Switch A</b> has a defined and enabled configuration. <b>Switch B</b> has a defined configuration but no enabled configuration.	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: cfg1	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: none	Configuration from <b>Switch A</b> propagates throughout the fabric. The configuration is enabled after the merge in the fabric.
<b>Switch A</b> and <b>Switch B</b> have the same defined configuration. Neither have an enabled configuration.	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: none	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: none	No change (clean merge).
<b>Switch A</b> and <b>Switch B</b> have the same defined and enabled configuration.	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: cfg1:	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: cfg1:	No change (clean merge).
<b>Switch A</b> does not have a defined configuration. <b>Switch B</b> has a defined configuration.	defined: none  enabled: none	defined:cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: none	<b>Switch A</b> absorbs the configuration from the fabric.
<b>Switch A</b> does not have a defined configuration. <b>Switch B</b> has a defined and enabled configuration.	defined: none  enabled: none	defined:cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: cfg1	<b>Switch A</b> absorbs the configuration from the fabric, with cfg1 as the enabled configuration.

TABLE 29 Zone merging scenarios: Defined and enabled configurations (continued)

Description	Switch A	Switch B	Expected results
<b>Switch A</b> and <b>Switch B</b> have the same defined configuration. Only <b>Switch B</b> has an enabled configuration.	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: none	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: cfg1	Clean merge, with cfg1 as the enabled configuration.
<b>Switch A</b> and <b>Switch B</b> have different defined configurations. Neither have an enabled configuration.	defined: cfg2 zone2: 10:00:00:90:69:00:00:8c; 10:00:00:90:69:00:00:8d  enabled: none	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: none	Clean merge. The new configuration will be a composite of the two.  defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  defined: cfg2 zone2: 10:00:00:90:69:00:00:8c; 10:00:00:90:69:00:00:8d  enabled: none
<b>Switch A</b> and <b>Switch B</b> have different defined configurations. <b>Switch B</b> has an enabled configuration.	defined: cfg2 zone2: 10:00:00:90:69:00:00:8c; 10:00:00:90:69:00:00:8d  enabled: none	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: cfg1	Clean merge. The new configuration is a composite of both, with cfg1 as the enabled configuration.
<b>Switch A</b> does not have a defined configuration.  <b>Switch B</b> has a defined configuration and an enabled configuration, but the enabled configuration is different from the defined configuration.	defined: none  enabled: none	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  effective: cfg1  zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  zone2: 10:00:00:90:69:00:00:8c; 10:00:00:90:69:00:00:8d	Clean merge. <b>Switch A</b> absorbs the defined configuration from the fabric, with cfg1 as the effective configuration.  In this case, however, the effective configurations for <b>Switch A</b> and <b>Switch B</b> are different. You should issue a <b>zoning enabled-configuration cfg-name</b> command from the switch with the proper effective configuration.

TABLE 30 Zone merging scenarios: Different content

Description	Switch A	Switch B	Expected results
Enabled configuration mismatch.	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b	defined: cfg2 zone2: 10:00:00:90:69:00:00:8c; 10:00:00:90:69:00:00:8d  enabled: cfg2 zone2: 10:00:00:90:69:00:00:8c; 10:00:00:90:69:00:00:8d	Fabric segments due to mismatching zone configurations
Configuration content mismatch.	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: irrelevant	defined: cfg1 zone1: 10:00:00:90:69:00:00:8c; 10:00:00:90:69:00:00:8d  enabled: irrelevant	Fabric segments due to mismatching zone content

TABLE 31 Zone merging scenarios: Different names

Description	Switch A	Switch B	Expected results
Same content, different enabled configuration name.	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b	defined:cfg2 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b	Fabric segments due to mismatching zone configurations

TABLE 31 Zone merging scenarios: Different names (continued)

Description	Switch A	Switch B	Expected results
	enabled: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b	enabled: cfg2 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b	
Same content, different zone name.	defined: cfg1 zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: irrelevant	defined: cfg1 zone2: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b  enabled: irrelevant	Fabric segments due to mismatching zone content
Same name, same content, different order.	defined: cfg1zone1: 10:00:00:90:69:00:00:8a; 10:00:00:90:69:00:00:8b; 10:00:00:90:69:00:00:8c  enabled: irrelevant	defined: cfg1zone1: 10:00:00:90:69:00:00:8b; 10:00:00:90:69:00:00:8c; 10:00:00:90:69:00:00:8a  enabled: irrelevant	Fabric segments due to mismatching zone content
Same name, different types.	effective: zone1: MARKETING	enabled: cfg1: MARKETING	Fabric segments due to mismatching types

TABLE 32 Zone merging scenarios: Default access mode

Description	Switch A	Switch B	Expected results
Different default zone access mode settings.	default zone: All Access	default zone: No Access	Clean merge. No Access takes precedence and default zone configuration from <b>Switch B</b> propagates to fabric.  default zone: No Access
Same default zone access mode settings.	default zone: All Access	default zone: All Access	Clean merge. Default zone configuration is All Access in the fabric.
Same default zone access mode settings.	default zone: No Access	default zone: No Access	Clean merge. Default zone configuration is No Access in the fabric.
Enabled zone configuration.	No enabled configuration. default zone = All Access	enabled: cfg2 default zone: All Access or No Access	Clean merge. Enabled zone configuration and default zone mode from <b>Switch B</b> propagates to fabric.
Enabled zone configuration.	No enabled configuration. default zone = No Access	enabled: cfg2 default zone: All Access	Fabric segments because <b>Switch A</b> has a hidden zone configuration (No Access) activated and <b>Switch B</b> has an explicit zone configuration activated.
Enable zone configuration.	enabled: cfg1 default zone: No Access	No enabled configuration. default zone: No Access	Clean merge. Enabled zone configuration from <b>Switch A</b> propagates to fabric.
Enable zone configuration.	enabled: cfg1 default zone: All Access	No enabled configuration. default zone: No Access	Fabric segments. You can resolve the zone conflict by changing the default zone to No Access on <b>Switch A</b> .

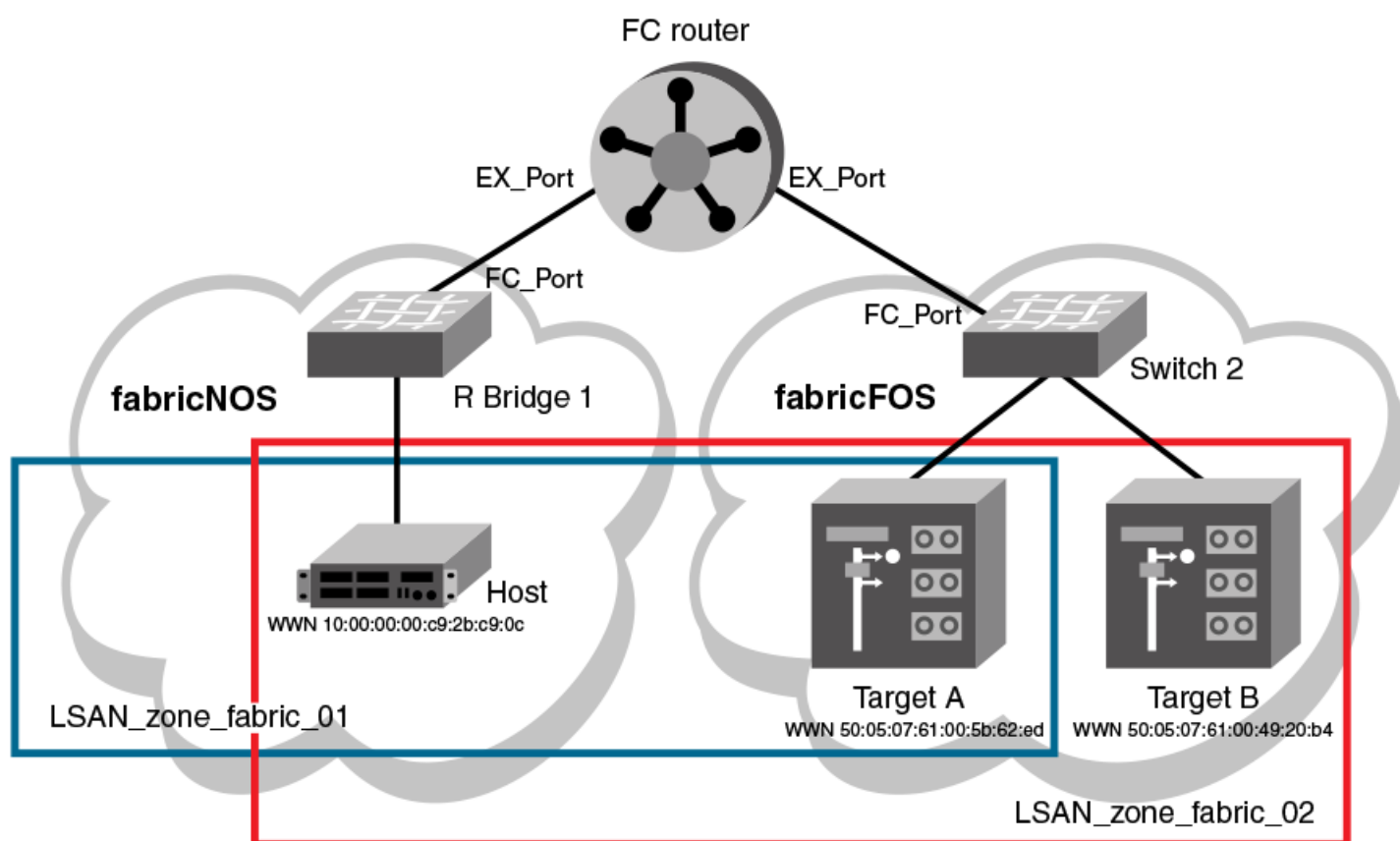
## Configuring LSAN zones: Device-sharing example

The following example shows LSANs sharing devices in separate fabrics. The procedure illustrates the creation of two LSAN zones (called `lsan_zone_fabric_02` and `lsan_zone_fabric_01`), which involve the following devices and connections:

- RBridge1 and the host in a Network OS fabric named fabric\_01.
- Switch2, Target A, and Target B in a Fabric OS fabric named fabric\_02.
- RBridge1 is connected by one of its FC\_Ports to an EX\_Port on the FC router.
- Switch2 is connected to the FC router using another EX\_Port or VEX\_Port.
- Host has WWN 10:00:00:00:c9:2b:c9:0c (connected to RBridge1).
- Target A has WWN 50:05:07:61:00:5b:62:ed (connected to switch2).
- Target B has WWN 50:05:07:61:00:49:20:b4 (connected to switch2).

The following illustration shows the connectivity.

FIGURE 31 LSAN zones example



The following example steps create this set of LSAN zones.

1. Obtain the host WWN in fabric\_01:
  - a) Log in to any switch in fabric\_01.
  - b) On the fabric\_01 switch, enter the **show name-server detail** command to list the WWN of the host (10:00:00:00:c9:2b:c9:0c).



**NOTE**

The **show name-server detail** output displays both the port WWN and node WWN; the port WWN must be used for LSANs.

```
switch# show name-server detail
PID: 012100
Port Name: 10:00:00:00:c9:2b:c9:0c
Node Name: 20:00:00:00:c9:2b:c9:0c
SCR: 3
FC4s: FCP
PortSymb: [27] "Brocade-1020|2.3.0.0|localhost.localdomain|Red Hat
Enterprise Linux Server release 5.5"
NodeSymb: NULL
Fabric Port Name: 20:21:00:05:1E:CD:79:7A
Permanent Port Name: 10:00:00:00:c9:2b:c9:0c
Device type: Physical Initiator
Interface: Fcoe 1/1/9
Physical Interface: Te 1/0/9
Share Area: No
Redirect: No
```

## 2. Obtain the target WWNS in fabric\_02:

- a) Log in as admin on switch2 in fabric\_02.
- b) On fabric\_02, enter the **nsShow** command to list Target A (50:05:07:61:00:5b:62:ed) and Target B (50:05:07:61:00:49:20:b4).

```
switch:admin> nsshows
{
Type Pid    COS  PortName                               NodeName                               TTL(sec)
NL  0508e8; 3;  50:05:07:61:00:5b:62:ed; 50:05:07:61:00:1b:62:ed; na
FC4s: FCP [IBM  DNEF-309170  F90F]
Fabric Port Name: 20:08:00:05:1e:34:11:e5
Permanent Port Name: 50:05:07:61:00:5b:62:ed

NL  0508ef; 3;  50:05:07:61:00:49:20:b4; 50:05:07:61:00:09:20:b4; na
FC4s: FCP [IBM  DNEF-309170  F90F]
Fabric Port Name: 20:08:00:05:1e:34:11:e5
Permanent Port Name: 50:05:07:61:00:49:20:b4
The Local Name Server has 2 entries }
```

3. Create an LSAN zone in the Network OS fabric (fabric\_01)
4. In fabric\_01, enter the **zoning defined-configuration zone** command to create the LSAN `lsan_zone_fabric_01`, and include the host.

```
switch# config terminal
switch(config)# zoning defined-configuration zone lsan_zone_fabric_01
switch(config-zone-lsan_zone_fabric_01)# member-entry 10:00:00:00:c9:2b:c9:0c
```

## 5. In fabric\_01, add Target A to the LSAN.

```
switch(config-zone-lsan_zone_fabric_01)# member-entry 50:05:07:61:00:5b:62:ed
switch(config-zone-lsan_zone_fabric_01)# exit
```

6. In fabric\_01, enter the **zoning defined-configuration cfg** and **zoning enabled-configuration cfg-name** commands to add and enable the LSAN configuration.

```
switch(config)# zoning defined-configuration cfg zone_cfg
switch(config-cfg-zone_cfg)# member-zone lsan_zone_fabric_01
switch(config-cfg-zone_cfg)# exit
switch(config)# zoning enabled-configuration cfg_name zone_cfg
```

Create an LSAN zone in the Fabric OS fabric (fabric\_02)

7. On switch2 (fabric\_02), enter the **zoneCreate** command to create the LSAN lsan\_zone\_fabric2, which includes the host (10:00:00:00:c9:2b:c9:0c), Target A (50:05:07:61:00:5b:62:ed) , and Target B (50:05:07:61:00:49:20:b4).

```
switch:admin> zonecreate "lsan_zone_fabric_02", "10:00:00:00:c9:2b:c9:0c;
                                         50:05:07:61:00:5b:62:ed;
                                         50:05:07:61:00:49:20:b4"
```

8. On switch2 (fabric\_02), enter the **cfgShow** command to verify that the zones are correct.

```
switch:admin> cfgshow
Defined configuration:
zone: lsan_zone_fabric_02
      10:00:00:00:c9:2b:c9:0c;
      50:05:07:61:00:5b:62:ed;
      50:05:07:61:00:49:20:b4
Effective configuration:
no configuration in effect
```

9. On switch2 (fabric\_02), enter the **cfgAdd** and **cfgEnable** commands to create and enable the LSAN configuration.

```
switch:admin> cfgadd "zone_cfg", "lsan_zone_fabric_02"
switch:admin> cfgenable "zone_cfg"
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected.
Do you want to enable 'zone_cfg' configuration (yes, y, no, n): [no] y
zone config "zone_cfg" is in effect
Updating flash ...
```

Display the configuration on the FC router:

10. Log in as an admin and connect to the FC router.  
11. On the FC router, enter the following commands to display information about the LSANs.

The **lsanZoneShow -s** command shows the LSAN.

```
switch:admin> lsanzoneshow -s
Fabric ID: 2 Zone Name: lsan_zone_fabric_02
 10:00:00:00:c9:2b:c9:0c Imported
 50:05:07:61:00:5b:62:ed EXIST
 50:05:07:61:00:49:20:b4 EXIST
Fabric ID: 75 Zone Name: lsan_zone_fabric_01
 10:00:00:00:c9:2b:c9:0c EXIST
 50:05:07:61:00:5b:62:ed Imported
```

The **fcrPhyDevShow** command shows the physical devices in the LSAN.

```
switch:admin> fcrphydevshow
Device      WWN                      Physical
Exists      PID
in Fabric
-----
 75          10:00:00:00:c9:2b:c9:0c   c70000
 2           50:05:07:61:00:49:20:b4   0100ef
 2           50:05:07:61:00:5b:62:ed   0100e8
Total devices displayed: 3
```

The **fcrProxyDevShow** command shows the proxy devices in the LSAN.

```
switch:admin> fcrproxydevshow
Proxy      WWN                      Proxy Device  Physical State
Created    PID Exists                PID
in Fabric
-----
 75          50:05:07:61:00:5b:62:ed 01f001   2           0100e8   Imported
 2           10:00:00:00:c9:2b:c9:0c 02f000   75          c70000   Imported
Total devices displayed: 2
```

On the FC router, the host and Target A are imported, because both are defined by `Isan_zone_fabric_02` and `Isan_zone_fabric_01`. However, target B is defined by `Isan_zone_fabric_02` and is not imported because `Isan_zone_fabric_01` does not allow it.



# Configuring Fibre Channel Ports

---

- [Fibre Channel ports overview](#).....181
- [Connecting to an FC Fabric through an FC Router](#).....182
- [Fibre Channel port configuration](#).....182

## Fibre Channel ports overview

Fibre Channel (FC) ports provide the ability to connect a Brocade VCS Fabric cluster to a Fibre Channel switch in a Fabric OS network.

The FlexPort feature is the only method that a switch running Network OS 5.0.0 or later can connect FC ports. For instructions on how to use FlexPort, refer to the "Configuring FlexPort" chapter of the *Network OS Layer 2 Switching Configuration Guide*.

The following platforms are Flexport-capable:

- Brocade VDX 2741
- Brocade VDX 2746
- Brocade VDX 6740
- Brocade VDX 6740T
- Brocade VDX 6740T-1G

These connections can be regular but not long distance. The following Network OS Fibre Channel port types are supported:

- E\_Port: Can be used to connect only to an EX\_Port on a FC SAN with Fibre Channel Routing configured.
- F\_Port:
  - Supports FC target connectivity (standards based F\_Port).
  - Supports bidirectional traffic internally from VF\_Port, or internal ISL port.

### NOTE

You must enable **fcoeport default** for the interface for the Fibre Channel logins to be available to connect to F\_Ports.

- Auto (G\_Port) — This is the default.
- N\_port:
  - Default port type in Access Gateway mode
  - Available in Access Gateway mode only
  - Supports bidirectional traffic internally from VF\_Port.
  - External connection to F\_Port on a FC SAN
- VF\_port:
  - For FCoE initiator or target connectivity.
  - Supports bidirectional traffic internally to E\_Port, F\_Port, VF\_Port (all in FCF mode), and N\_Port (in AG mode).

FC ports can connect to a FC switch in a Fabric OS network through two methods:

- Using an Inter-Switch Link (ISL) connection from an FC E\_port on a Flexport-capable switch to a FC router's EX\_Port; this in turn connects to the FC switch in the Fabric OS network. The VDX FC ports are configured as E\_Ports for this connection. Refer to [Connecting to an FC Fabric through an FC Router](#) on page 182.
- Using a direct connection from an FC port on a Flexport-capable switch to an F\_Port on a FC router in a Fabric OS network. The VDX FC ports are configured as N\_Ports through the Access Gateway feature. Refer to [Access Gateway](#) on page 189.

## Connecting to an FC Fabric through an FC Router

FC ports on Flexport-capable switches can provide a connection to a FC switch in the FC SAN.

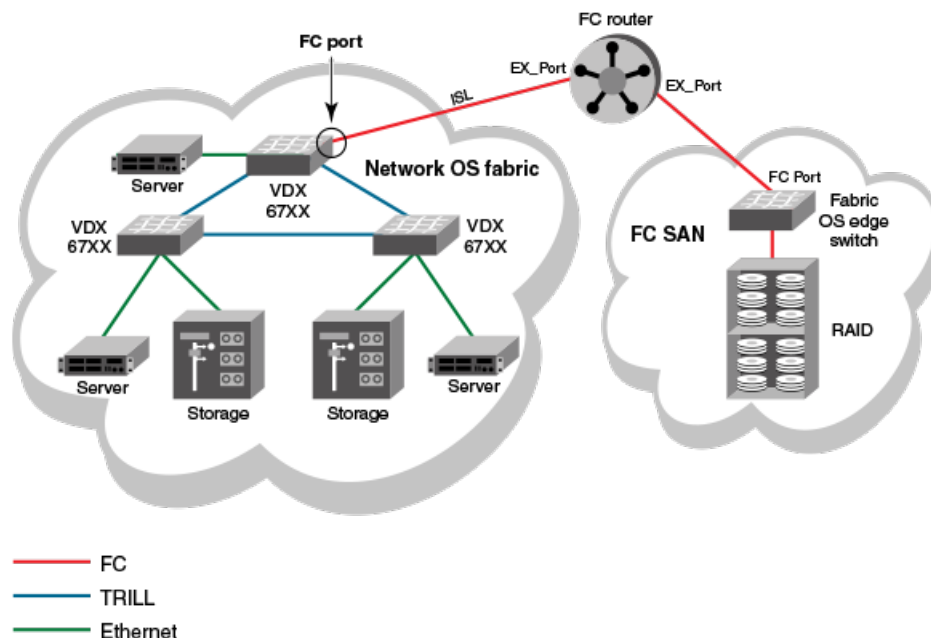
The FC ports on the Flexport-capable switch can be configured as FC E\_Ports to connect with EX\_Ports on a FC router through Inter-Switch Links (ISL) links. In turn, EX\_Ports on the FC router connect to F\_Ports on the FC Fabric switch. These connections provide support for zoning across Network OS and Fabric OS fabric types, which can enable FCoE devices on the Brocade VCS Fabric cluster to access SAN storage and services. Refer to [Fibre Channel ports overview](#) on page 181 for information on how to create LSAN zones.

The following figure shows an FC connection between a Network OS fabric and Fibre Channel SAN.

### NOTE

For details of Fibre Channel routing concepts, refer to the *Fabric OS Administrator's Guide*

FIGURE 32 FC connection between a Network OS fabric and a Fibre Channel SAN



## Fibre Channel port configuration

Consider the topics discussed below when configuring Fibre Channel ports.

### Using Fibre Channel commands

Network OS software provides the following high-level commands for managing Fibre Channel ports:

- **interface FibreChannel** - Global configuration mode command that allows you to enter the interface Fibre Channel configuration submode where you can enter commands to activate and deactivate a Fibre Channel port (**no shutdown** and **shutdown** commands) and to set port attributes (**desire-distance**, **fill-word**, **isl-r\_rdy**, **speed**, **trunk-enable**, and **vc-link-init** commands).
- **show running-config interface FibreChannel** - A privileged EXEC mode command that displays Fibre Channel port configuration information.

- **show interface FibreChannel** - A privileged EXEC mode command that displays hardware counters that monitor activity and status of a Fibre Channel port.

## Activating and deactivating Fibre Channel ports

When VCS mode is enabled and an FCoE license is installed, all FC ports are activated by default. When enabling a switch for Access Gateway Mode, all FC ports are re-enabled as N\_Ports.

### Prerequisites for enabling Fibre Channel ports

Follow these steps before enabling a Fibre Channel port.

1. An FCoE license must be installed on the FlexPort-capable switch to allow Fibre Channel port activation. Refer to the *Network OS Software Licensing Guide* for details about installing the FCoE license. Once the FCoE license is installed, all Fibre Channel ports are activated by default.
2. The FlexPorts on the switch must be configured as fibre channel ports. For instructions on how to use FlexPort, refer to the "Configuring FlexPort" chapter of the *Network OS Layer 2 Switching Configuration Guide* and to the applicable hardware guides.

#### NOTE

Access Gateway is a feature available only on FlexPort-capable switches. When activated, all Fibre Channel ports are re-enabled as N\_Ports.

### Enabling a Fibre Channel port

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **interface FibreChannel** *rbridge-id/slot/port* command for the Fibre Channel port you want to enable.

#### NOTE

You do not to be in RBridge ID configuration mode to disable or enable a Fibre Channel port. It is recommended that you configure this on the principal switch.

A configuration submenu prompt appears.

3. Enter the **no shutdown** command.

The following example enables port 1 in slot 0 of RBridge ID 8.

```
switch# configure terminal
switch(config)# interface FibreChannel 8/0/1
switch(config-if-fi-8/0/1)# no shutdown
```

### Disabling a Fibre Channel port

1. In privileged EXEC mode, enter the **configure terminal** command to enter the global configuration mode.
2. Enter the **interface FibreChannel** *rbridge-id/slot/port* command for the Fibre Channel port you want to disable.

A configuration submenu prompt appears.

3. Enter the **shutdown** command.

The following example disables port 1 in slot 0 of RBridge ID 8.

```
switch# configure terminal
switch(config)# interface FibreChannel 8/0/1
switch(conf-if-fi-8/0/1)# shutdown
```

## Configuring and viewing Fibre Channel port attributes

This section introduces the options for configuring a variety of Fibre Channel port attributes and confirming the status of those attributes.

### Using Fibre Channel port commands

Network OS v2.1.1 and later allows you to configure and display the following attributes for a Fibre Channel port by using the commands shown below:

- Port speed — Enter the interface Fibre Channel configuration submode **speed** command to set the speed of a Fibre Channel port.
- Trunk port — Enter the interface Fibre Channel configuration submode **trunk-enable** command to configure the port for trunking.
- Buffer credit control — Enter the interface Fibre Channel configuration submode **isl-r\_r-rdy** command to enable interswitch link receiver-ready (ISL R\_RDY) mode on the port. Enter the interface Fibre Channel configuration submode **no isl-r\_r-rdy** command to disable ISL R\_RDY mode on the port. If ISL R\_RDY is not set, then Inter-SwitchLink Virtual Channel ready (ISL VC\_RDY) mode is set by default.
- Forward error correction — **fec-enable** is set by default for 16G FC port speeds; use **no fec-enable** to disable this capability.
- FC port type restriction — **config-mode** allows the following possible completions:
  - auto — Configures the port as a G-Port (locked).
  - eport — Configures the port as a E-Port (locked).
  - fport — Configures the port as a F-Port (locked).
  - nport — Configures the port as a N-Port (locked).
- Port group speed — The hardware connector group-speed configuration allows you to set the allowed speed ranges and protocol type for groups of FlexPorts.

#### ATTENTION

Setting ISL R\_RDY is not recommended.

The following Fibre Channel port attributes are not supported by Network OS 5.0.0 or later:

AL_PA offset 13	F_Port buffers	Persistent Disable
Compression	Fault Delay	Port Auto Disable
Credit Recovery	Frame shooter port	QoS E_Port
CSCTL mode	Locked L_Port	Rate limit
D-Port mode	LOS TOV enable	RSCN suppressed
Disabled E_Port	Mirror Port	
Encryption		
EX_Port		



## Viewing Fibre Channel port attributes

To view the Fibre Channel port attributes for a single port, in privileged EXEC mode, enter the **show running-config interface FibreChannel *rbridge-id/slot/port*** command for the port you want to view. To view the Fibre Channel port attributes for all Fibre Channel ports in the fabric, enter the **show running-config interface FibreChannel** command without any additional parameters.

Whether you view attributes for a single port or for all ports, the settings for the **isl-r\_rdy**, **trunk-enable**, and **shutdown** attributes are always displayed. The **fec-enable** and **speed** attributes are displayed only if they are set to nondefault values.

The following example displays the Fibre Channel port attributes for a single port. In this case, the **speed** and **vc-link-init** attributes appear because they have been set to values other than their default values.

```
switch# show running-config interface FibreChannel 8/0/1
interface FibreChannel 8/0/1
  speed 8gbps
  no isl-r_rdy
  trunk-enable
  shutdown
```

The following example shows Fibre Channel attributes for all Fibre Channel ports. In this case, the **speed** and **fec-enable** attributes are set to their default values for all of the interfaces shown.

```
switch# show running-config interface FibreChannel
interface FibreChannel 3/0/1
  desire-distance 0
  no isl-r_rdy
  trunk-enable
  no shutdown
!
interface FibreChannel 3/0/2
  no isl-r_rdy
  trunk-enable
  no shutdown
!
interface FibreChannel 3/0/3
  no isl-r_rdy
  trunk-enable
  no shutdown
!
      (output truncated)
```

To view the setting of a single attribute on a specific port, regardless of whether the attribute is set to its default value, enter the **show running-config interface FibreChannel *rbridge-id/slot/port*** command.

The following example shows the setting of the speed attribute for port 66/0/1:

```
switch# show running-config interface FibreChannel 66/0/1 speed interface FibreChannel 66/0/1
speed 16gbps
```

## Setting Fibre Channel port speed

This procedure sets the ports speed to 4, 8, or 16 Gbps, or to autonegotiate (the default value).

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **interface FibreChannel *rbridge-id/slot/port*** command for the port on which you want to set the speed.

A configuration submenu prompt appears.

3. Enter the **speed** command followed by the desired speed in Gbps.

The following example sets the port speed to 4 Gbps.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface FibreChannel 8/0/1
switch(config-FibreChannel-8/0/1)# speed 4
```

## Configuring a Fibre Channel port for trunking

A link can be configured to be part of a trunk group. Two or more links in a port group form a trunk group when they are configured for the same speed, the same distance level, and their link distances are nearly equal.

1. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
2. Enter the **interface FibreChannel** *rbridge-id/slot/port* command for the desired port.  
A configuration submenu prompt appears.
3. Enter the **trunk-enable** command.

The following example configures the link attached to port 4 on RBridge 8 to be part of a trunk group.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# rbridge-id 8
switch(config-rbridge-id-8)# interface FibreChannel 8/0/4
switch(config-FibreChannel-8/0/4)# trunk-enable
```

## Monitoring Fibre Channel ports

To monitor a Fibre Channel port, in privileged EXEC mode, enter the **show interface FibreChannel** *rbridge-id/slot/port* command for the Fibre Channel port you want to monitor. The command output provides lots of information about the various hardware counters associated with the port.

This command has a basic version and a detail version. The basic version of the command provides general port information such as status, identification, and configuration information, along with interrupt statistics, link status counters, and so on, as shown in the following example:

```
switch# show interface FibreChannel 66/0/1

fibrechannel 66/0/1 is down (No_Light). Protocol state is down.
Pluggable media present
LineSpeed Actual:
PortSpeed:                N8Gbps
portDisableReason:        Persistently disabled port
PortId:                    010000
PortIfId:                  43010000
PortWwn:                   20:00:00:27:f8:d4:79:be
Distance:                  normal
FEC:                       Inactive

Last clearing of show interface counters: 00:00:00
Interrupts:                0          Link_failure: 0          Frjt:          0
Unknown:                   0          Loss_of_sync: 0          Fbsy:          0
Lli:                       0          Loss_of_sig:  0
Proc_rqrd:                 0          Protocol_err: 0
Timed_out:                 0          Invalid_word: 0
Rx_flushed:                0          Invalid_crc:  0
Tx_unavail:                0          Delim_err:    0
Free_buffer:               0          Address_err:  0
Overrun:                   0          Lr_in:        0
Suspended:                 0          Lr_out:       0
Parity_err:                0          Ols_in:       0
2_parity_err:              0          Ols_out:      0
CMI_bus_err:               0

Rate info:
  Bandwidth:                8.00G
  Tx performance:          0 B/sec
  Rx performance:          0 B/sec
```

The detailed version of the command, illustrated below, tells you how much traffic has been transmitted or received, and how many times certain error conditions have occurred. Specifically, the `tim_tocrd_z` counters tell you how many times the port was unable to transmit frames because the transmit BB credit was zero. A number greater than zero indicates either that there is congestion on the port or that a device is affected by latency. A larger number indicates a greater problem. A sample is taken every 2.5 microseconds.

```
switch# show interface FibreChannel 66/0/1 detail

fibrechannel 66/0/1 is down (No_Light). Protocol state is down.
Pluggable media present
LineSpeed Actual:
PortSpeed:                N8Gbps
portDisableReason:        Persistently disabled port
PortId:                    010000
PortIfId:                  43010000
PortWwn:                   20:00:00:27:f8:d4:79:be
Distance:                  normal
FEC:                       Inactive

Last clearing of show interface counters: 00:00:00
Rx Statistics:
  stat_wrx                0          4-byte words received
  stat_frx                0          Frames received
Tx Statistics:
  stat_wtx                0          4-byte words transmitted
  stat_ftx                0          Frames transmitted
Error Statistics:
  er_enc_in               0          Encoding errors inside of frames
  er_crc                  0          Frames with CRC errors
  er_trunc                 0          Frames shorter than minimum
  er_toolong              0          Frames longer than maximum
  er_bad_eof               0          Frames with bad end-of-frame
  er_enc_out               0          Encoding error outside of frames
  er_bad_os                0          Invalid ordered set
  er_crc_good_eof         0          Crc error with good eof

Port Error Info:
  loss_of_sync:           0
  lossofsig:              0
  frjt:                   0
  fbsy:                   0

Buffer Information:
  Lx      Max/Resv  Buffer  Needed  Link  Remaining
  Mode   Buffers   Usage  Buffers Distance Buffers
=====
  -       8         0      0      -     0

Rate info:
  Bandwidth:              8.00G
  Tx performance:         0 B/sec
  Rx performance:         0 B/sec
```



# Access Gateway

---

• Access Gateway basic concepts.....	189
• Enabling Access Gateway mode.....	199
• Disabling Access Gateway mode.....	199
• Displaying Access Gateway configuration data.....	200
• VF_Port to N_Port mapping.....	202
• Port Grouping policy.....	205
• Trunking in Access Gateway mode.....	211
• Access Gateway under FlexPort.....	212
• N_Port monitoring for unreliable links.....	213
• Displaying Access Gateway N_Port utilization data .....	214

## Access Gateway basic concepts

Access Gateway (AG) simplifies server and storage connectivity by enabling direct connection of servers to any SAN fabric—enhancing scalability by eliminating the switch domain identity and simplifying local switch device management.

On supported switches, the Access Gateway (AG) feature enables you to configure FC ports as N\_Ports and to map specific VF ports to these N\_Ports. This allows direct connection of hosts attached to the VF\_Ports on the AG-supported switch with F\_Ports on a Fibre Channel fabric edge switch instead of through ISL connections to a Fibre Channel Router (FCR). These connections can be regular or long distance.

Through the use of N\_Ports for direct connection to FC switches and VF\_Port to N\_Port mapping, Access Gateway provides the following benefits:

- As ISLs between switches and FCRs utilize possibly limited domain IDs to identify switches, direct connection from AG-switch N\_Ports to Fibre Channel switch F\_Ports can resolve scalability issues, as the number of Fibre Channel and VCS fabrics grow.
- Direct connection from AG-switch N\_Ports to F\_Ports allows greater interoperability with multivendor Fibre Channel fabrics, as connection to these fabrics through an FCR is limited.
- The use of N\_Ports instead of ISL connections to FCRs increases the number of device ports available for FCoE hosts and devices behind LAG-supported FSBs connected to the AG-switch VF\_Ports. In addition, through use of N\_Port ID Virtualization (NPIV), multiple FCoE initiators can access the SAN through the same physical port.

After you configure a switch in AG mode, all FC Ports are enabled as N\_Ports. These ports connect to F\_Ports on the FC fabric. If the AG switch is connected to a FC switch, the connected N\_Ports should come up automatically. Devices attached to VF\_Ports come up when FCoE is enabled on Ethernet ports.

## Switches supported for Access Gateway

From Network OS 7.0.0, the following Brocade switches support Access Gateway:

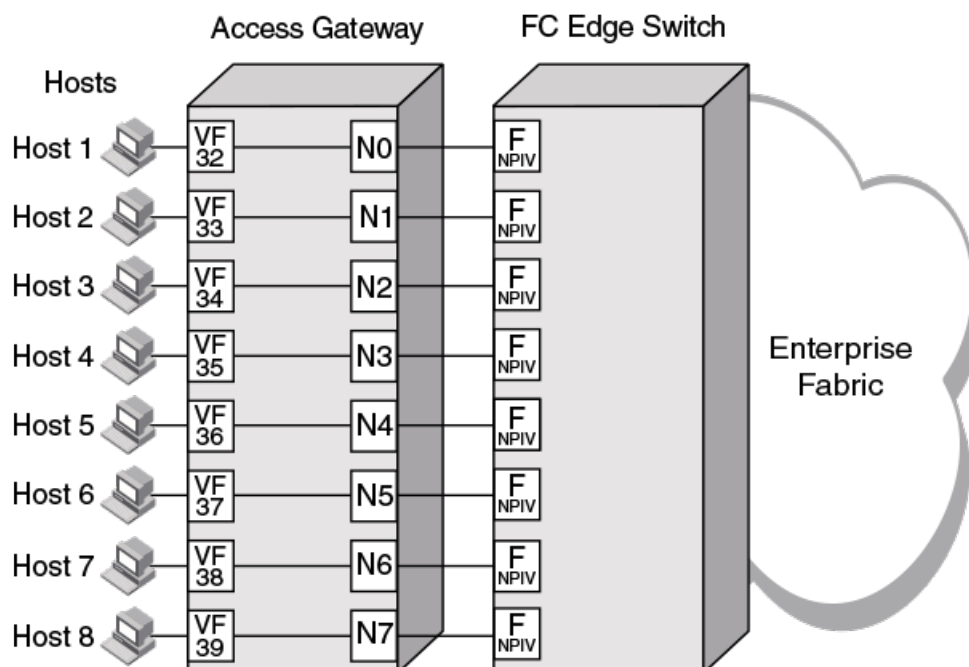
- VDX 6740, VDX 6740T, and VDX 6740T-1G
- VDX 2741
- VDX 2746

## Network diagrams

The following diagrams illustrate various connection configurations among switches and network elements, with and without Access Gateway.

The following figure illustrates the connection of eight hosts through an AG switch to a Fibre Channel fabric edge switch.

FIGURE 33 Hosts connecting to FC fabric through switch in AG mode

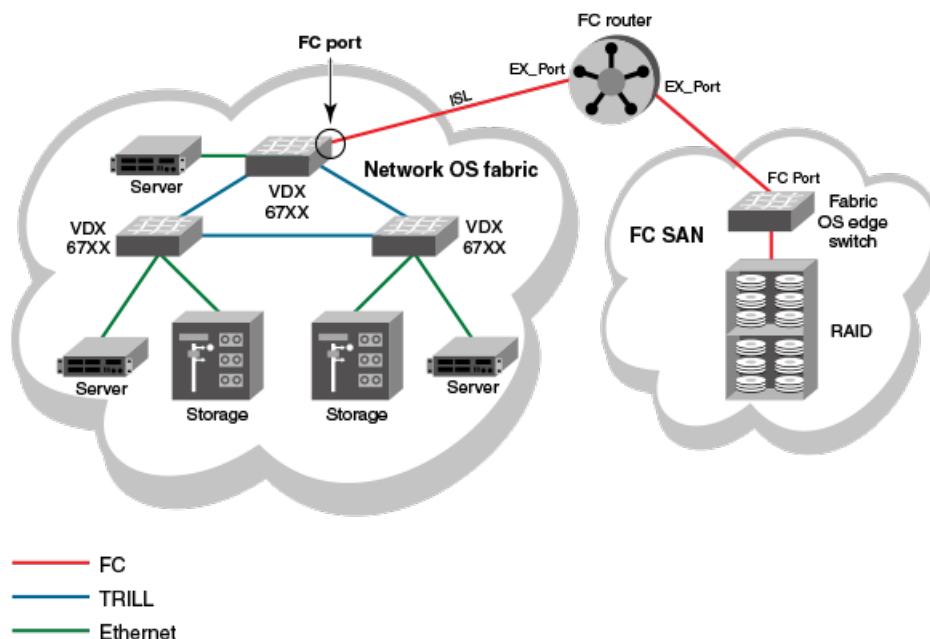


### NOTE

An AG switch can connect to only one Fibre Channel SAN. Ports on this switch connecting to a second FC SAN are disabled. Multiple AG switches, each belonging to a different VCS cluster, can connect to the same SAN fabric.

The following figure illustrates an alternate connection of hosts (servers) to an FC fabric through a switch not in Access Gateway mode. A VDX FC port, configured as an E\_Port, connects to the FC SAN through an ISL connection to an FC router. For more information on configuring FC ports for an ISL and FC router connection, refer to [Configuring Fibre Channel Ports](#) on page 181.

FIGURE 34 Connecting Network OS fabric to FC fabric without AG mode



Switches in AG mode are logically transparent to the host and the fabric. Therefore, you can increase the number of hosts that have access to the fabric without increasing the number of switch domains. This simplifies configuration and management in a large fabric by reducing the number of domain IDs and ports.

VCS mode must be enabled to enable Access Gateway on the switch. By default, both VCS mode and AG are enabled.

While in AG mode, the switch functions both as a VCS and AG switch as follows:

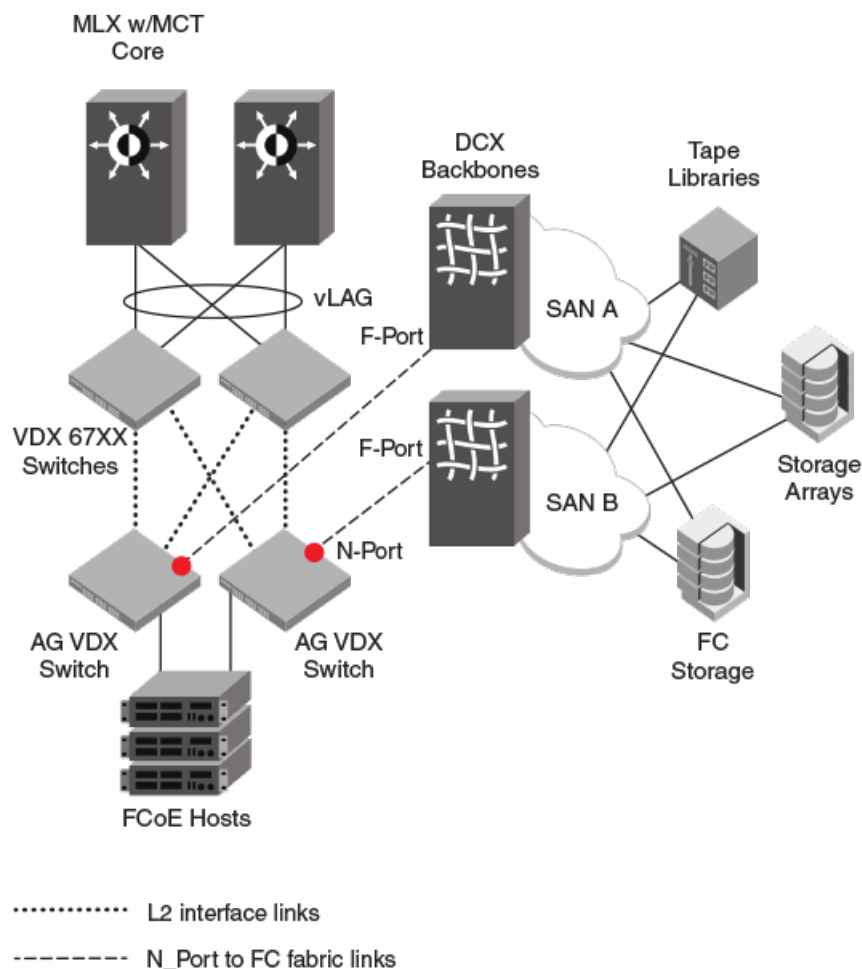
- It supports N\_Ports, VF\_Ports, and Layer 2 interfaces.
- It can connect devices to a VCS fabric through Ethernet ports. VCS fabric services run on Ethernet ports which function under the "native" VCS switch configuration.
- It can connect hosts to a Fibre Channel switch through VF\_Ports mapped to N\_Ports.

#### NOTE

In this document, VCS native (or native) mode refers to a switch enabled in VCS mode. Access Gateway mode (or AG switch) refers to a switch in VCS mode enabled for the Access Gateway feature.

The following figure illustrates the connection of FCoE hosts to two AG switches in a top-of-rack configuration. N\_Ports on these switches connect to F\_Ports on Brocade DCX Backbones in the FC SAN. In addition, Layer 2 interfaces on these switches connect to other VDX switches in the VCS fabric cluster.

FIGURE 35 Using Access Gateway to connect FC and VCS fabrics



## Access Gateway and native VCS modes

In native VCS mode, the switch can function as part of a VCS Fabric cluster, but cannot connect to a FC fabric through N\_Ports. When enabled in AG mode, the switch can still function as part of a VCS Fabric cluster, but can now connect directly with a FC "edge" fabric switch through F\_Port to N\_Port connections.

All VCS and Network OS features are available to a switch in AG mode, which is enabled by default. If you need to enable AG mode (for example, if upgrading from a legacy version), use the **enable** command.

For more information enabling and disabling AG mode, refer to [Enabling Access Gateway mode](#) on page 199 and [Disabling Access Gateway mode](#) on page 199.



## Access Gateway in a logical chassis cluster

Although operations of a VDX switch configured in Access Gateway mode are similar to a node configured in native VCS mode while in Logical Chassis Cluster mode, there are some unique considerations that you should be aware of.

Nodes in a logical chassis cluster are configured in Logical Chassis Cluster mode. In this mode, both the data and configuration paths are distributed to other nodes in the cluster. The entire cluster is configured from the principal node. For more information, refer to [Logical chassis cluster mode](#) on page 58.

Behavior and operations of an Access Gateway node configured in a logical chassis cluster, such as removing the node from or adding the node to the cluster, are similar to operations in other nodes in the cluster. Access Gateway does not have any global configuration, so the default configuration for the node in Access Gateway mode is similar to a cluster node in native VCS mode. Failover in the cluster, both controlled and uncontrolled, also occurs the same as for an AG switch.

There are two methods for adding an Access Gateway node to the cluster:

- You can enable Access Gateway on a standalone switch, then add the switch to the cluster. Before adding the switch, enable it for Access Gateway mode and configure Access Gateway features and policies through the Network OS AG commands. The node you add to the cluster must have same VCS ID as the cluster; otherwise the configuration on the node will revert to default configuration.
- You can enable Access Gateway on a switch that is already a node in the cluster by just enabling AG on the switch.

## Access Gateway with FCoE logical SANs

Access Gateways play a central role in supporting the FCoE Logical SANs feature, and require special configuration.

Logical SANs can be configured as either local or remote. A local SAN provides logical separation within the VCS Fabric, while a remote SAN provides Fibre Channel SAN connectivity through an Access Gateway in the fabric. The Access Gateway provides connectivity to only one logical SAN, while other switches in the fabric can be configured to support multiple logical SANs.

For an overview of the role of Access Gateways in this feature and how to configure them, refer to the chapter "Configuring FCoE Logical SANs" in the *Network OS Layer 2 Switching Configuration Guide*.

## Access Gateway ports

Access Gateway supports VF\_Ports that connect host systems to the switch, Layer 2 interface ports that connect the switch to the VCS Fabric cluster, and FC N\_Ports that connect the switch to a FC fabric.

In order for hosts attached to VF\_Ports on a VDX switch to connect with F\_Ports on a FC switch, the VF\_Ports must be mapped to the VDX switch N\_Ports. Enabling AG mode configures all FC ports as N\_Ports and maps VF\_Ports to the N\_Ports in a sequential, round-robin fashion. This allows for even distribution of logins in a typical configuration, where VF\_Ports are sequentially allocated as ENodes log in. You can change this default mapping by mapping any VF\_Port to an N\_Port using Network OS commands, as described in [Configuring port mapping](#) on page 203.

The following types of ports are supported on a VDX switch in AG mode:

- N\_Ports (node ports)—Connects a switch in AG mode to the F\_Port on the Fibre Channel switch. By using FlexPort commands, you can enable the following numbers of N\_Ports on supported switches:
  - VDX 6740 — 32 N\_Ports
  - VDX 6740T — 16 N\_Ports
  - VDX 6740T-1G — 16 N\_Ports
  - VDX 2741 — 16 external ports and 16 (4 x 4) ports in breakout mode. Ethernet is supported, but Fibre Channel is not supported.
  - VDX 2746 — 14 external ports and 8 (2 x 4) ports in breakout mode

- VF\_Ports (Virtual Fabric ports)—Connect FCoE hosts and devices behind LAG-supported FSB devices. You can map these ports to specific N\_Ports for connection to a Fibre Channel switch. Consider the following specifications:
  - By default, each switch is assigned 64 VF\_Ports.
  - There is no limit to the number of VF\_Ports that you can map to an N\_Port.
  - Up to 64 NPIV logins are allowed per VF\_Port.
  - Valid VF\_Port numbers are 1 to 1000.
- L2 interface ports—Ethernet TRILL ports that connect with other VDX switches in the Brocade VCS Fabric cluster. The number of available TRILL ports = (total number of physical ports) - (ports converted to Fibre Channel ports).

Since all VDX switch FC ports are enabled as N\_Ports in Access Gateway mode, FC hosts or targets cannot directly attach to the AG switch. When Access Gateway mode is enabled, you can configure additional FC port attributes for the N\_Ports as you would on non-AG switches.

### Transitioning from native VCS to AG mode

Be aware of the following interface and port functions after enabling AG mode:

- CEE interfaces will be in a no-shutdown state.
- If FC ports are connected to FC switch F\_Ports, connected N\_Ports should come up automatically. Devices connected to mapped VF\_Ports should come up after you enter the **fcoeport** command on the interface port.
- VDX switch Ethernet ports are under the native VCS switch configuration.
- For default VF\_Port to N\_Port mapping, VF\_Ports are mapped to N\_Ports sequentially in a round-robin fashion as ENodes log in. Mapping that you implement through the **map fport interface fcoe port** command overrides the default mapping.
- VCS Fabric services run on VCS ports and not under the Access Gateway daemon.

### Comparison of Access Gateway, ISL, and FC switch ports

A switch in Access Gateway (AG) mode uses VF\_Ports and N\_Ports to connect devices to the Fibre Channel (FC) switch. The connected FC switch connects to the AG switch N\_Ports through F\_Ports and presents a variety of ports for connection to FC fabric devices.

Access Gateway (AG) multiplexes host connections to the fabric. AG presents a VF\_Port to a FCoE host and an N\_Port to an edge Fibre Channel fabric switch. Multiple VF\_Ports mapped to N\_Ports provide multiple device ports for connection to the FC fabric.

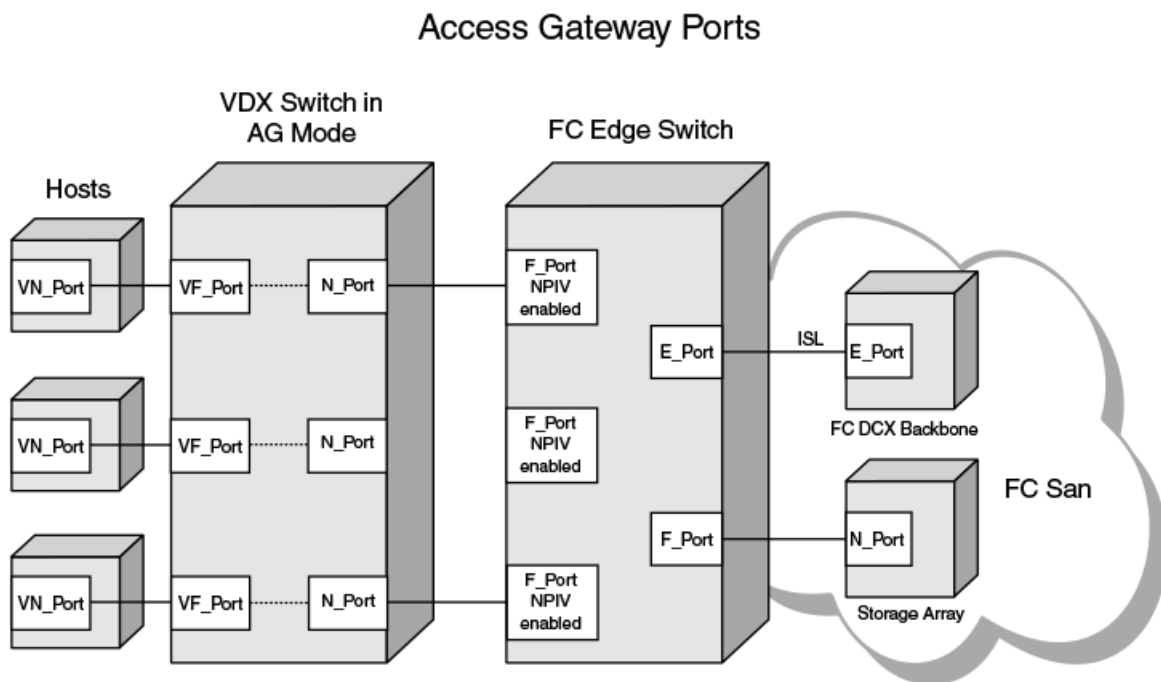
Using N\_Port ID Virtualization (NPIV), AG allows multiple FCoE initiators to access the SAN on the same physical port. This reduces the hardware requirements and management overhead of hosts to the SAN connections.

In contrast to the AG switch, the connected FC switch presents F\_Ports (or FL\_Ports) to storage devices hosts and presents E\_Ports, VE\_Ports, or EX\_Ports to other switches in the fabric.

A native switch using an ISL connection between its FC E\_Port and an EX\_Port on an FCR consumes domain ID resources that may impact scalability as VCS and FC fabrics grow. In addition, connection through a FCR may limit connection to multivendor FC fabrics. Finally, connection through an ISL provides limited device port connections to the FC fabric. For more information on configuring FC ports for connection to an FCR and FC fabric, refer to [Configuring Fibre Channel Ports](#) on page 181.

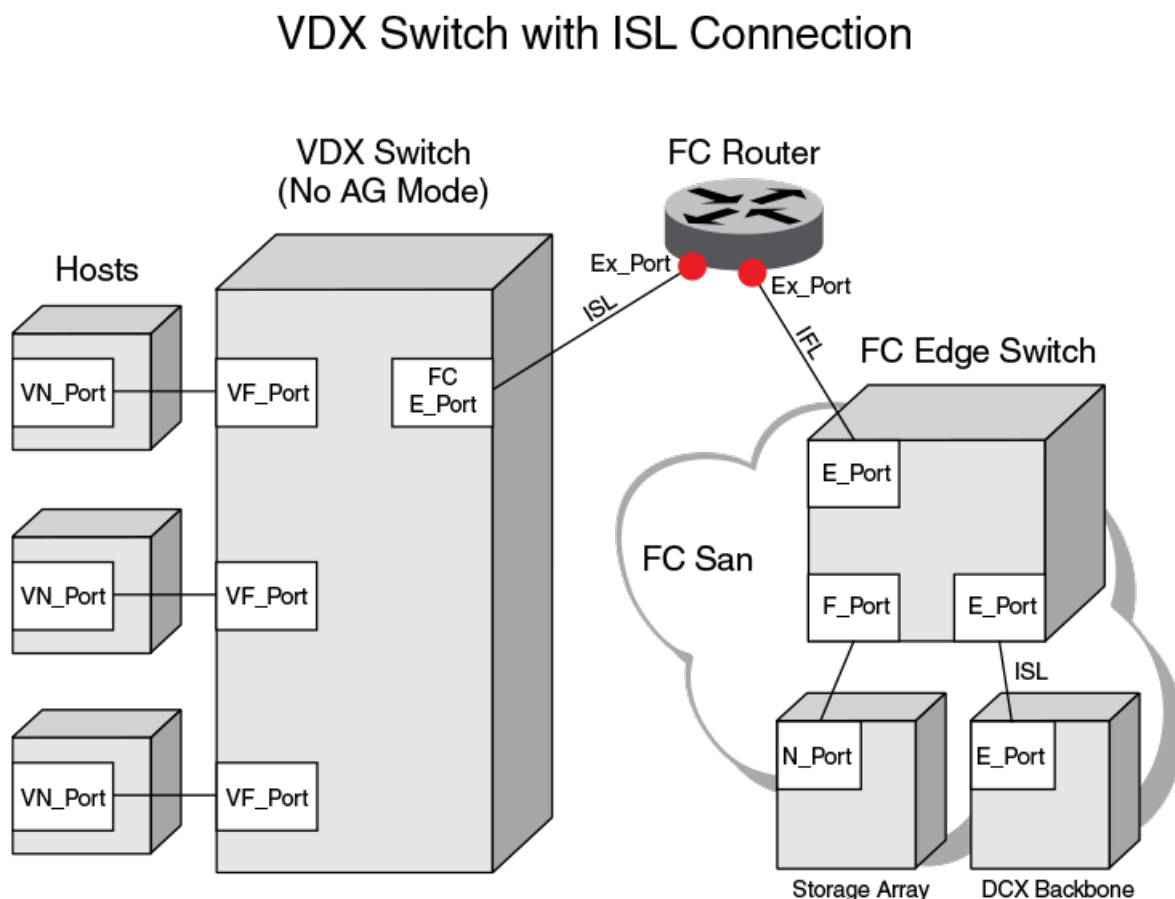
The following figure illustrates ports used for connecting hosts attached to an Access Gateway Switch to a Fibre Channel switch.

FIGURE 36 Access Gateway and FC switch ports



The following figure illustrates the ports used for connecting hosts attached to a non-AG (native) switch to a Fibre Channel switch, using an ISL connection.

FIGURE 37 Connection of native VCS and FC ports



## Access Gateway features and requirements

Although Access Gateway provides standard features for connection to Fibre Channel SANs, you can configure a number of optional features as well. There are also requirements and limitations that you should be aware of when using this feature in a VCS cluster and FC fabric environment.

### Port grouping

The Port Grouping (PG) policy is enabled by default when AG is enabled. This allows you to group N\_Ports into a port group. By default, any VF\_Ports mapped to these N\_Ports are also members of that port group. Port Grouping allows you to isolate specific hosts to specific FC fabric ports for performance, security, or other reasons.

Automatic Login Balancing (LB) and Modified Managed Fabric Name Monitoring (M-MFNM) modes are enabled by default when the PG policy is enabled.

- When LB mode is enabled and an N\_Port goes offline, existing logins from VF\_Ports that are mapped to the offline N\_Port are distributed to available N\_Ports in the port group. If a new N\_Port comes online, existing logins are not disturbed. LB mode can be disabled using Network OS commands.
- When LB mode is disabled, VF\_Ports are not shared among N\_Ports in the port group, as VF\_Ports can only connect to N\_Ports to which they are mapped. As a best practice to ensure device login, bind the ENode to a VF\_Port and ensure that its mapped N\_Port is online.

- M-MFNM mode ensures that all N\_Ports connect to the same FC fabric, preventing connections to multiple SANs. M-MFNM cannot be disabled as long as LB mode is enabled.

For more information on Port Grouping policy modes, refer to [Port Grouping policy modes](#) on page 209.

## N\_Port monitoring for unreliable links

The N\_Port monitoring for unreliable links feature monitors links from all N\_Ports on the VDX switch to F\_Ports on the FC fabric. If online and offline static change notifications (SCNs) exceed a set threshold during a specific time period, the link is considered unreliable, and the N\_Port is taken offline. The VF\_Ports mapped to the N\_Port also go offline. If the N\_Port is in a port group and Automatic Login Balancing is enabled, the VF\_Ports mapped to the N\_Port are distributed among available N\_Ports in the same port group.

## Additional features and functions

Following are additional features and functions of Access Gateway:

- Access Gateway enables VDX FC ports as N\_Ports. Hosts attached to VDX VF\_Ports can connect directly with F\_Ports on a Fibre Channel fabric edge switch through these N\_Ports.
- Instead of using ISL connections and possibly limited domain resources, the use of N\_Ports increases the number of available device ports on the switch. As the number of Fibre Channel and VCS Fabrics grow, scalability is less of an issue.
- Through the use of N\_Port ID Virtualization (NPIV), multiple FCoE initiators can access the SAN through the same physical port.
- When enabling AG mode, VF\_Ports are mapped to available N\_Ports in a round-robin fashion as ENodes log in. However, you can re-map any VF\_Port to switch N\_Ports.
- Access Gateway can operate in both fabric cluster and logical chassis cluster modes.
- You can configure additional FC port attributes for the AG switch N\_Ports as you would on non-AG switches. Refer to [Configuring Fibre Channel Ports](#) on page 181

## Limitations

Following are limitations you should be aware of when using Access Gateway mode:

- Hosts connected to an Access Gateway switch cannot communicate with targets on the VCS Fabric.
- A VDX switch configured for Access Gateway can connect with only one FC Fabric. Ports connected to a second FC fabric are disabled.
- Access Gateway can operate in both fabric cluster mode and logical chassis cluster modes. The AG configuration is not distributed in fabric cluster mode and is distributed in logical chassis cluster mode.
- You can only configure VF\_Port to N\_Port mapping for devices directly attached to VF\_Ports and F\_Ports on the connected FC switch. These mappings control device logins through appropriate N\_Ports.
- Since all switch FC ports are configured as N\_Ports when AG mode is enabled:
  - FC hosts or targets cannot be directly attached to the AG switch.
  - The AG switch cannot be connected to a Fabric OS Access Gateway in a Cascaded configuration.
- Access Gateway does not "bridge" the VCS and FC fabrics:
  - Hosts connected to VF\_Ports mapped to Access Gateway N\_Ports appear on the FC fabric only.
  - Device FC IDs are assigned by the FC fabric F\_Ports connected to the Access Gateway N\_Ports.
  - VF\_Ports and N\_Ports are under the Access Gateway daemon's configuration.
  - Fibre Channel OS components, such as management server, name server, and zoning are restricted on Network OS Access Gateways just as they are on Fabric OS Access Gateways. Refer to the *Fabric OS Access Gateway Administrator's Guide* for a complete list.

- Although the **show fcoe login** command displays FCoE devices connected to the Access Gateway switch VF\_Ports, these devices are in the FC fabric and cannot be detected by the VCS Fabric name server. Therefore, these devices cannot be zoned in a VCS Fabric.

## FCoE and Layer 2 support and limitations

The following functions are supported:

- The following functionality is supported for a configuration consisting of a vLAG from a host CNA to two Access Gateway switches or to an AG switch and a VCS Switch (L2 vLAG for top of rack split):
  - The vLAG links can carry Layer 2 and Layer 3 traffic.
  - VLAG support is identical to support in native VCS mode.
  - A separate FCoE device login is supported through each AG switch.
- The following functionality is supported for a configuration with a LAG from an FSB to an AG switch:
  - LAG specifics, such as number of links and contiguous vs. discontinuous, is identical to native VCS support.
  - Multiple LAGs can connect to the AG switch (one per FSB).
  - LAG carries Layer 2 and Layer 3 traffic.
  - Devices connected via an FSB LAG cannot talk to a Cisco SAN.
  - LAGs and direct attached devices are supported on the same AG switch.
- The following functionality is supported for VF\_Ports and CEE interfaces:
  - VF\_Ports are dynamically bound to Ethernet interfaces as in native VCS mode.
  - As in native VCS mode, all CEE interfaces with connected devices must be configured for FCoE.
  - The CEE interface will come up as an ISL ET port if it is connected to a peer ET port on another switch in the VCS Fabric.
  - As in native VCS mode, 64 VF\_Ports are allocated by default.
  - A VF\_Port can accept up to 64 NPIV logins.
  - As in native VCS mode, VF\_Ports are dynamically allocated as devices come up.
  - As in native VCS mode, VF\_Ports can be statically bound to ENodes.
  - VCS Fabric services run on VCS ports and not under Access Gateway.
  - As in native VCS mode, the number of VF\_Ports allocated can be changed dynamically:
    - > You can configure the maximum number of FCoE devices that can be logged into a switch by using the **fcoe\_enodes** command.
    - > Newly allocated VF\_Ports are mapped to existing N\_Ports sequentially in a round-robin fashion, which assigns all VF\_Ports sequentially and evenly to the N\_Ports.
    - > Newly deallocated VF\_Ports are removed from existing VF\_Port to N\_Port mappings.

Following are support limitations:

- If an interface is only handling L2 traffic, the corresponding VF\_Port appears as disabled to AG.
- For vLAGs:
  - As in native VCS mode, a vLAG with FSB cannot support FCoE traffic. It can support L2 traffic only.
  - A vLAG from a host Converged Network Adapter (CNA) supports L2 and FCoE traffic.
- A single LAG/link is supported between one FSB and one AG switch. Subsequent LAG/links are treated as a TRILL loop and disabled.
- LAG member VF\_Ports cannot be mapped to individual N\_Ports or N\_Port groups.
- The **enable** command is not allowed if the RBridge is part of an FCoE forwarder (FCF)-group as an FCF-RBridge ID (rbid) in an FCoE fabric-map configuration.
- The **no enable** command is not allowed if the RBridge contains a port provisioned for FCoE.

## Enabling Access Gateway mode

Enabling Access Gateway (AG) mode on a VDX switch allows FCoE hosts and devices behind LAG-supported FSBs connected to VF\_Ports to connect to a FC fabric.

### NOTE

On supported devices, Access Gateway mode is enabled by default.

Enabling AG mode enables FC ports on the switch, configuring them as N\_Ports. The N\_Ports can connect directly to F\_Ports on an edge FC switch. VF\_Ports are mapped to N\_Ports in a sequential, round-robin fashion as Enodes log in. You can change this default mapping using Network OS commands.

### NOTE

Before enabling or disabling AG mode, ensure that the following conditions are fulfilled:

- All Fibrechannel interfaces are in shut state.
- There are no ports provisioned for FCoE.
- The RBridge ID of the switch is not specified in the FCoE forwarder (FCF) configuration.

Use the following procedure to enable Access Gateway mode.

1. Enter the **configure terminal** command to change to global configuration mode.

```
device# configure terminal
```

2. Enter the **rbridge-id** command, specifying the RBridge ID.

```
device(config)# rbridge-id 1
```

3. Enter the **ag** command to change to AG configuration mode.

```
device(config-rbridge-id-1)# ag
```

4. Enter the **enable** command.

```
device(config-rbridge-id-1-ag)# enable
```

AG mode is enabled. Switch FC ports are automatically enabled as N\_Ports and mapped to VF\_Ports.

### NOTE

You can configure additional FC port attributes for the N\_Ports as you would on switches in native mode. Refer to [Configuring Fibre Channel Ports](#) on page 181.

## Disabling Access Gateway mode

Disabling Access Gateway (AG) mode returns the switch to native VCS mode. Disabling AG mode also removes all AG configuration, including port mapping and N\_Port configuration.

### NOTE

Before enabling or disabling AG mode, ensure that the following conditions are fulfilled:

- All Fibrechannel interfaces are in shut state.
- There are no ports provisioned for FCoE.
- The RBridge ID of the switch is not specified in the FCoE forwarder (FCF) configuration.

Use the following procedure to disable AG mode on the switch.

1. Display the current AG state and configuration by entering the **show ag rbridge-id** *rbridge-id* command in privileged EXEC mode.

```
device# show ag rbridge-id 1
```

If Access Gateway configuration data displays, as shown in [Displaying Access Gateway configuration data](#) on page 200, AG is enabled.

If "AG mode not set" displays as shown in the following example, AG is not enabled.

```
device# show ag rbridge-id 2
AG mode not set.
```

For more information on displaying the current AG configuration on a switch or all AG switches in a VCS cluster using this command, refer to [Displaying Access Gateway configuration data](#) on page 200.

2. Enter the **configure terminal** command to change to global configuration mode.

```
device# configure terminal
```

3. Enter the **rbridge-id** command, specifying the RBridge ID.

```
device(config)# rbridge-id 1
```

4. Enter the **ag** command to change to AG configuration mode.

```
device(config-rbridge-id-1)# ag
```

5. Disable AG mode by entering the **no enable** command.

```
device(config-rbridge-id-1-ag)# no enable
```

## Displaying Access Gateway configuration data

Use the **show running-config rbridge-id** *rbridge id* **ag** and **show ag rbridge-id** *rbridge-id* commands to display Access Gateway configuration data.

To display AG configuration data, use the following methods:

- Use the **show running-config rbridge-id** *rbridge-id* **ag** command to display the configured N\_Port to VF\_Port mappings, port grouping information, and other parameters. This shows the factory-default configuration, unless parameters have been modified by the user.
- Use the **show ag rbridge-id** *rbridge-id* command to display the current and active status of AG configuration, such as the switch identification, number and type of ports, enabled policies, port grouping, and attached fabric details. This displays only ports that are currently online and current mappings. For example, this will show VF\_Ports that have failed over to an N\_Port if an N\_Port that has gone offline.

### NOTE

Display of current, active mapping, or configured mapping for a port group using the **show ag rbridge-id** *rbridge-id* and **show running-config rbridge-id** *rbridge-id* **ag** commands depends on the enabled or disabled state of Login Balancing mode. For more information, refer to [Automatic Login Balancing mode](#) on page 209.

1. Make sure you are in Privileged EXEC mode and have a switch prompt such as the following.

```
switch#
```

2. Perform one of the following steps:



- Enter the **show running-config rbridge-id *rbridge-id* ag** command as in the following example for RBridge 1.

```
switch# show running-config rbridge-id 1 ag
```

- Enter the **show ag rbridge-id *rbridge-id*** command as shown in the following example for RBridge 5.

```
switch# show ag rbridge-id 5
```

If Access Gateway is enabled, data such as the following displays for **show running-config rbridge-id *rbridge-id* ag**, as shown in the following example for RBridge 1:

```
device# show running-config rbridge-id 1 ag
rbridge-id 1
  ag
    enable
    counter reliability 25
    timeout fnm 120
    nport interface FiberChannel 1/0/1
      map fport interface Fcoe 1/1/1 1/1/2 1/1/3 1/1/4 1/1/5 1/1/6 1/1/7 1/1/8 1/1/9 1/1/10 1/1/11 1/1/12 1/1/13
1/1/14 1/1/15 1/1/16 1/1/17 1/1/18 1/1/19 1/1/20 1/1/21 1/1/22 1/1/23 1/1/24 1/1/25 1/1/26 1/1/27 1/1/28 1/1/29
1/1/30 1/1/31 1/1/32 1/1/33 1/1/34 1/1/35 1/1/36 1/1/37 1/1/38 1/1/39 1/1/40 1/1/41 1/1/42 1/1/43 1/1/44 1/1/45
1/1/46 1/1/47 1/1/48 1/1/49 1/1/50 1/1/51 1/1/52 1/1/53 1/1/54 1/1/55 1/1/56 1/1/57 1/1/58 1/1/59 1/1/60 1/1/61
1/1/62 1/1/63 1/1/64
    !
    nport interface FiberChannel 1/0/2
    !
  pg 0
    nport interface FibreChannel 1/0/1 1/0/2
    modes lb
    rename pg0
    !
  !
!
```

If Access Gateway is enabled, data such as the following displays for **show ag rbridge-id *rbridge-id***, as shown in the following example for RBridge 1:

```
device# show ag rbridge-id 1
Rbridge-ID 1:
-----
Name                : device
NodeName            : 10:00:00:27:f8:cf:9b:b8
Number of Ports     : 128
IP Address(es)      : 11.11.11.11
Firmware Version    : v6.0.1
Number of N_Ports(Fi) : 1
Number of VF_Ports  : 1
Policies Enabled    : pg
Port Group information :
PG_IDPG_NamePG_ModePG_Members
-----
0          pg0      lb      1/0/1, 1/0/2
-----
Fabric Information :
Attached Fabric NameN_Ports(Fi)
-----
10:00:00:05:33:ae:8a:87 1/0/2
-----
N_Port(Fi) information :
Port      PortID      Attached PWWN      IP_Addr      VF_Ports
-----
Fi 1/0/2      0x010200      2f:03:00:05:33:ae:8a:87      11.11.11.11      1/1/1
-----
VF_Port information :
VF_Port   Eth_Port   PortID   Attached PWWN      N_Port(Fi)
-----
1/1/1     Te 1/0/25   0x010201 10:00:00:05:1e:d4:88:be      1/0/2
```

```

1/1/1    Te 1/0/25    0x010202  77:77:77:77:77:77:00  1/0/2
1/1/1    Te 1/0/25    0x010203  77:77:77:77:77:77:01  1/0/2
1/1/1    Te 1/0/25    0x010204  77:77:77:77:77:77:02  1/0/2
1/1/1    Te 1/0/25    0x010205  77:77:77:77:77:77:03  1/0/2

```

If AG is not enabled, "AG mode not set" displays, as shown in the following example for RBridge 2:

```

device# show ag rbridge-id 2
AG mode not set.

```

#### NOTE

You can also enter **show ag rbridge-id all** to display AG configuration data for all switches in the VCS cluster.

## VF\_Port to N\_Port mapping

To connect hosts attached to VDX Switch VF\_Ports to Fibre Channel switch F\_Ports, the appropriate VF\_Ports must be mapped to VDX Switch N\_Ports. Although ports have a factory-default mapping based on the VDX platform, you can change mapping using Network OS commands.

Consider the following when mapping ports:

- You can map multiple VF\_Ports to an N\_Port. There is no limit to the number of VF\_Ports that you can map to an N\_Port.
- You can only configure VF\_Port to N\_Port mapping for devices directly attached to VF\_Ports on the VDX switch and F\_Ports on the connected FC switch. These mappings control device logins through appropriate N\_Ports.
- Consider the N\_Port and VF\_Port ranges allowed for a VDX platform. Refer to [Access Gateway ports](#) on page 193.
- If an N\_Port is removed from a port group enabled for Automatic Login Balancing mode and moved to another port group, the VF\_Ports mapped to that N\_Port remain with the N\_Port. If an N\_Port is moved from a port group not enabled for Automatic Login Balancing mode, the VF\_Ports that are mapped to the N\_Port move to the default Port Group 0.

## Displaying port mapping

You can display current and configured VF\_Port to N\_Port mapping on a specific switch or on all switches enabled for Access Gateway in the VCS cluster.

Display current, active VF\_Port to N\_Port mapping on a specific switch or on all switches enabled for Access Gateway in the VCS cluster using the **show ag map rbridge-id rbridge-id** command while in Privileged EXEC mode.

Display configured VF\_Port to N\_Port mapping on a switch using the **show running-config rbridge-id rbridge id ag** command.

Perform one of the following steps while in privileged EXEC mode:

- To display current, active, VF\_Port mapping for a specific N\_Port, enter **show ag map nport rbridge-id rbridge-id**.

```

switch# show ag map nport interface fiberChannel 200/0/1 rbridge-id 200

```
- To display current, active VF\_Port mapping to all N\_Ports on a switch, enter **show ag map rbridge-id rbridge-id**.

```

switch# show ag map rbridge-id 200

```
- To display VF\_Port mapping to a N\_Ports on all switches in the VCS cluster, enter **show ag map rbridge-id all**.

```

switch# show ag map rbridge-id all

```
- To display configured mapping on a switch, enter **show running-config rbridge-id rbridge id ag**.

```

switch# show running-config rbridge-id 1 ag

```

## Current and configured mapping display

Display of current, active mapping, or configured mapping for a port group using the **show ag map** and **show running-config rbridge-id rbridge id ag** commands depend on the enabled or disabled state of Login Balancing mode. For more information, refer to [Automatic Login Balancing mode](#) on page 209.

The following example is sample output from the **show ag map rbridge-id rbridge-id** command, which shows current, active port mapping. The "Current\_VF\_Ports" column shows that there are no VF\_Ports online.

```
switch# show ag map rbridge 5
RBridge-ID 5:
-----
N_Port(Fi)    PG_ID  PG_Name  Current_VF_Ports
-----
5/0/1         0      pg0      None
5/0/2         0      pg0      None
5/0/3         0      pg0      None
5/0/4         0      pg0      None
5/0/5         0      pg0      None
5/0/6         0      pg0      None
5/0/7         0      pg0      None
5/0/8         0      pg0      None
-----
```

The following example is sample output from the **show running-config rbridge-id rbridge id ag** command to show configured port mapping. The output lists N\_Port numbers on the switch, and then mapped VF\_Ports following "map fport interface fcoe."

```
switch# show running-config rbridge-id 1 ag
rbridge-id 1
ag
  nport 1/0/1
    map fport interface Fcoe 1/1/1 1/1/9 1/1/17 1/1/25 1/1/33 1/1/41 1/1/49 1/1/57
    !
  nport 1/0/2
    map fport interface Fcoe 1/1/2 1/1/10 1/1/18 1/1/26 1/1/34 1/1/42 1/1/50 1/1/58
    !
  nport 1/0/3
    map fport interface Fcoe 1/1/3 1/1/11 1/1/19 1/1/27 1/1/35 1/1/43 1/1/51 1/1/59
    !
  nport 1/0/4
    map fport interface Fcoe 1/1/4 1/1/12 1/1/20 1/1/28 1/1/36 1/1/44 1/1/52 1/1/60
    !
  nport 1/0/5
    map fport interface Fcoe 1/1/5 1/1/13 1/1/21 1/1/29 1/1/37 1/1/45 1/1/53 1/1/61
    !
  nport 1/0/6
    map fport interface Fcoe 1/1/6 1/1/14 1/1/22 1/1/30 1/1/38 1/1/46 1/1/54 1/1/62
    !
  nport 1/0/7
    map fport interface Fcoe 1/1/7 1/1/15 1/1/23 1/1/31 1/1/39 1/1/47 1/1/55 1/1/63
    !
  nport 1/0/8
    map fport interface Fcoe 1/1/8 1/1/16 1/1/24 1/1/32 1/1/40 1/1/48 1/1/56 1/1/64
    !
  pg 0
    nport interface FibreChannel 1/0/1 1/0/2 1/0/3 1/0/4 1/0/5 1/0/6 1/0/7 1/0/8
    modes lb
    rename pg0
    !
  timeout fnm 120
  counter reliability 25
```

## Configuring port mapping

When operating in Access Gateway mode, you can specify routes that AG will use to direct traffic from the devices (hosts or targets) on its VF\_Ports to the ports connected to the fabric using its N\_Ports. The process of specifying routes is called "mapping." When AG is

enabled on a switch, VF\_Ports are assigned to available N\_Ports in a round-robin fashion as ENodes log in. You can change this mapping using the following instructions.

Use the **map fport interface fcoe *port*** command to map specific VF\_Ports to a an N\_Port to ensure that all traffic from these VF\_Ports always goes through the same N\_Port. You must enter this command while in N\_Port configuration mode for a specific N\_Port. All VF\_Ports mapped to an N\_Port in an N\_Port group will be part of that port group.

Remember the following points when mapping ports:

- The range of valid VF\_Ports and N\_Ports is specific to the VDX platform. Refer to [Access Gateway ports](#) on page 193 for valid port numbers.
- Newly allocated VF\_Ports are mapped to existing N\_Ports in a round-robin fashion.
- Newly deallocated VF\_Ports are removed from existing mappings.
- If the AG switch is connected to a FC switch, the connected N\_Port and devices on the mapped VF\_Ports should come online automatically.

Use the following steps to configure VF\_Port to N\_Port mapping:

1. Perform steps under [Displaying port mapping](#) on page 202 to display current and configured port mapping.
2. Enter the **configure** command to access global configuration mode.

```
switch# configure
```

3. Enter the **rbridge-id *id*** command to enter RBridge ID mode for the specific switch.

```
switch(config)# rbridge-id 2
```

4. Enter the **ag** command to enter Access Gateway configuration mode.

```
switch(config-rbridge-id-2)# ag
```

5. Enter the **nport interface fiberchannel *port*** command for the N\_Port where you want to change or set mapping to a VF\_Port, where *port* is the N\_Port number in rbridge-id/slot/port format. This accesses the configuration mode for the N\_Port.

```
switch(config-rbridge-id-2-ag)# nport interface fiberchannel 2/0/4
```

6. Perform one of the following steps:

- To map a VF\_Port to the N\_Port, enter **map fport interface fcoe *port***, where *port* is the VF\_Port in domain/rbridge-id/port format.

```
switch(config-rbridge-id-2-ag-nport-if-fi-2/0/4)# map fport interface fcoe 1/2/26
```

- To remove a VF\_Port mapped to the N\_Port, enter the **no map fport interface fcoe *port*** command, where *port* is the VF\_Port number in domain/rbridge-id/port format.

```
switch(config-rbridge-id-2-ag-nport-if-fi-2/0/4)# no map fport interface fcoe 1/2/26
```

7. Return to privileged EXEC mode and enter the **show running-config rbridge-id *rbridge id* ag** command to verify configured VF\_Port to N\_Port mapping. Refer to [Displaying port mapping](#) on page 202 for more information.

```
switch# show running-config rbridge-id 2 ag
```

## Port Grouping policy

The Port Grouping (PG) policy partitions the VF\_Ports, host, target ports within an Access Gateway-enabled switch into independently operated groups. Port Grouping allows you to dedicate specific hosts to specific fabric ports for performance, security, or other reasons.

Port Grouping policy is enabled by default when you enable Access Gateway mode and cannot be disabled.

To create port groups, you group N\_Ports under a specific port group ID. By default, any VF\_Ports mapped to the N\_Ports belonging to a port group are members of that port group. All N\_Ports in the group are shared by all VF\_Ports mapped to those N\_Ports. ENodes can log in as long as an online N\_Port exists in the group.

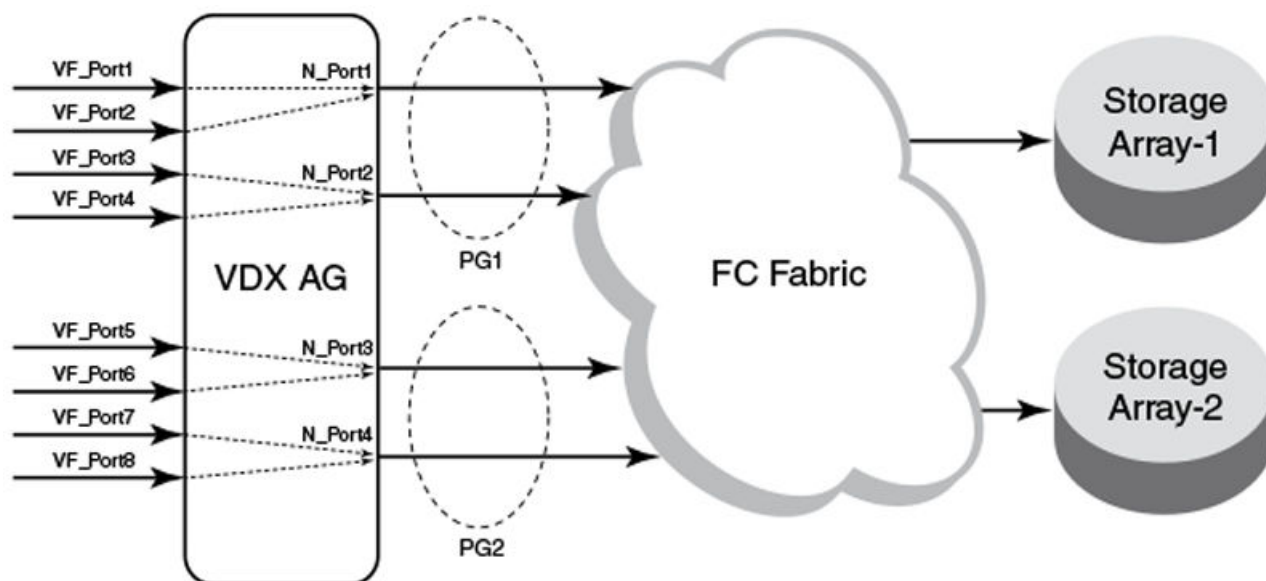
### NOTE

In Network OS commands, N\_Ports are designated by the format `rbridge-id/port group/N_Port`. For example, `5/O/1` designates RBridge 5/port group 1/N\_Port 1.

When Access Gateway mode is enabled, a default port group 0 (pg 0) is created that contains all N\_Ports on the switch. The maximum number of port groups supported is 16, including pg 0.

The following figure illustrates two port groups connecting VF\_Ports to an FC fabric. Ports in PG 1 are connecting to one storage array, while ports in PG2 are connecting to a different storage array.

**FIGURE 38** Port groups connecting to FC fabric



Following are considerations and limitations for the Port Grouping policy.

- An ENode can log in.
- A port cannot be a member of more than one port group.
- The PG policy is enabled by default in when you enable AG mode. A default port group "0" (PG0) is created, which contains all N\_Ports and mapped VF\_Ports on the switch.
- If an N\_Port is added to a port group or deleted from a port group, it maintains its original mapping configuration. If an N\_Port is deleted from a port group, it is automatically added to port group 0.

## Displaying port grouping information

Display information for N\_Port groups configured on the switch or all switches in the VCS cluster enabled for Access Gateway mode. Access Gateway must be enabled for this command to succeed.

Use the **show ag pg rbridge-id** *rbridge id* command while in Privileged EXEC mode to display information on N\_Port groups configured on a switch. This information includes N\_Ports and VF\_Ports in the group and enabled PG modes.

1. Configure port groups using steps under [Creating and removing port groups](#) on page 206.
2. Perform one of the following steps while in Privileged EXEC mode:
  - To display the current information for port groups on a specific switch, enter **show ag pg rbridge-id** *rbridge-id*.

```
switch# show ag pg rbridge-id 5
```

- To display port grouping information for port groups on all Access Gateway switches in the VCS cluster, enter **show ag pg rbridge-id all**.

```
switch# show ag pg rbridge-id all
```

- To display current information on a specific port group (such as pg 11), enter **show ag pg pgid** *rbridge-id* *rbridge-id*.

```
switch# show ag pg pgid 11 rbridge-id 200
```

The following is an example of command output for RBridge 5:

```
switch# show ag pg rbridge-id 5
Rbridge-ID 5:
-----
PG_ID  PG_Name  PG_Mode  N_Ports (Fi)                VF_Ports
-----
    0   pg0      1b      5/0/1, 5/0/2, 5/0/3, 5/0/4,  1/5/1, 1/5/2, 1/5/3, 1/5/4,
      5/0/5, 5/0/6, 5/0/7, 5/0/8  1/5/5, 1/5/6, 1/5/7, 1/5/8,
                                     1/5/9, 1/5/10, 1/5/11, 1/5/12,
                                     1/5/13, 1/5/14, 1/5/15, 1/5/16,
                                     1/5/17, 1/5/18, 1/5/19, 1/5/20,
                                     1/5/21, 1/5/22, 1/5/23, 1/5/24,
                                     1/5/25, 1/5/26, 1/5/27, 1/5/28,
                                     1/5/29, 1/5/30, 1/5/31, 1/5/32,
                                     1/5/33, 1/5/34, 1/5/35, 1/5/36,
                                     1/5/37, 1/5/38, 1/5/39, 1/5/40,
                                     1/5/41, 1/5/42, 1/5/43, 1/5/44,
                                     1/5/45, 1/5/46, 1/5/47, 1/5/48,
                                     1/5/49, 1/5/50, 1/5/51, 1/5/52,
                                     1/5/53, 1/5/54, 1/5/55, 1/5/56,
                                     1/5/57, 1/5/58, 1/5/59, 1/5/60,
                                     1/5/61, 1/5/62, 1/5/63, 1/5/64
-----
```

## Creating and removing port groups

You must create a port group with a unique ID before adding N\_Ports to the group or enabling Port Grouping (PG) policy modes. Removing a port group removes all N\_Ports, mapped VF\_Ports, and associated PG modes.

Access Gateway must be enabled for the **pg** command to succeed.

When you enable Access Gateway mode, all ports belong to port group 0 (pg0). You can move ports to a separate port group by first creating a port group with a unique ID, and then adding N\_Ports to that group. All VF\_Ports mapped to added N\_Ports also become members of the new group. Removing a port group removes all N\_Ports, mapped VF\_Ports, and associated PG modes.

Use the **pg** *pgid* command to configure a port group with a unique ID (*pgid*). The *pgid* is a number that cannot exceed the number of N\_Ports allocated for the switch model, minus 1 for default pg 0. Therefore, for a VDX with 16 N\_Ports, a valid *pgid* would be from 1

through 15. Once configured, you can access the port group for configuration tasks, such as adding and removing N\_Ports, enabling port group modes, and renaming the group. Use the **no pg *pgid*** command to remove a port group. You enter these commands while in Access Gateway (ag) configuration mode.

#### NOTE

Port Grouping policy is enabled by default when you enable Access Gateway mode.

1. Enter the **configure** command to enter global configuration mode.

```
switch# configure
```

2. Enter the **rbridge-id *id*** command to enter RBridge ID mode for the specific switch.

```
switch(config)# rbridge-id 3
```

3. Enter the **ag** command to enter Access Gateway configuration mode.

```
switch(config-rbridge-id-3)# ag
```

4. Perform one of the following steps:

- To create a port group, enter the **pg *pgid*** command.

```
switch(config-rbridge-id-3-ag)# pg 1
```

- To remove a port group, enter the **no pg *pgid*** command.

```
switch(config-rbridge-id-3-ag)# no pg 1
```

Creating a port group with the **pg *pgid*** command enters the PG configuration mode for the port group ID (*pgid*) so that you can add N\_Ports and perform other PG policy configuration.

```
switch(config-rbridge-id-3-ag-pg-1)#
```

5. Verify that the port group was created using the **show ag pg *pgid* rbridge-id *rbridge-id*** command from privileged EXEC configuration mode. Refer to [Displaying port grouping information](#) on page 206 for details.

## Naming a port group

You can name or rename a port group and use this name in place of the port group ID.

Access Gateway and the PG policy must be enabled for the **rename** command to succeed.

Use the **rename *pgid*** command while in the configuration mode for a port group to change the port group name. The name cannot exceed 64 characters.

1. Enter the **configure** command to enter global configuration mode.

```
switch# configure
```

2. Enter the **rbridge-id *rbridge-id*** command to enter RBridge ID configuration mode for the specific switch.

```
switch(config)# rbridge-id 3
```

3. Enter the **ag** command to enter Access Gateway configuration mode.

```
switch(config-rbridge-id-3)# ag
```

- Enter the port group ID, such as pg 1, to enter configuration mode for the port group.

```
switch(config-rbridge-id-3-ag)# pg 1
```

- Change the name of the port group using the **rename** *pgid* command. In the following example, port group is named pg-array24.

```
switch(config-rbridge-id-3-ag-pg-1)# rename pg-array24
```

The port group name must not exceed 64 characters.

## Adding and removing N\_Ports in a port group

After creating a port group, you must add N\_Ports to the group. You must delete N\_Ports from a group if you want to move them to another port group or not include them in a port group.

Access Gateway and the PG policy must be enabled for the **nport interface fibrechannel** command to succeed.

Use the **nport interface fibrechannel** *port* command while in command mode for a specific port group to add an N\_Port to the group. Use the **no nport interface fibrechannel** *port* command to remove an N\_Port. Before you can add a port to a port group, you must remove it from the port group where it currently exists, unless the port is in port group 0 (pg 0). If you remove a port from a port group, it will default to port group 0. You cannot delete a port from port group 0.

### NOTE

Under FlexPort, after you move a VF\_Port from one port group to another, it is possible that an N\_Port may not be available in the target port group.

- Determine the port group on the switch where the port is currently a member by entering the **show ag pg rbridge-id** *rbridge-id* while in the privileged EXEC command mode.

```
switch# show ag pg rbridge-id 3
```

- Enter the **configure terminal** command to enter global configuration mode.

```
switch# configure terminal
```

- Enter the **rbridge-id** command to enter rbridge ID configuration mode.

```
switch(config)# rbridge-id 3
```

- Enter the **ag** command to enter Access Gateway command mode.

```
switch(config-rbridge-id-3)# ag
```

- Enter the port group ID, such as pg 1, to enter configuration mode for the port group where the N\_Port currently resides.

```
switch(config-rbridge-id-3-ag)# pg 1
```

- To delete the N\_Port from the group, use the **no nport interface fibrechannel** *port* command. In the following example, N\_Port 3 is removed from port group 1.

Before deleting the N\_Port, all VF\_Ports mapped to the N\_Port should be remapped. If the port resides in port group 0 (pg 0), you do not need to remove it from the port group before adding it to a different port group and can skip to the next step.

```
switch(config-rbridge-id-3-ag-pg-1)# no nport interface fibrechannel 3/0/3
```

You can delete multiple N\_Ports by listing the ports separated by spaces as in the following example.

```
no nport interface fibrechannel 3/0/3 3/0/5
```



- Enter the configuration mode for port group ID where you want to add the port, for example pg 2.

```
switch(config-rbridge-id-3-ag)# pg 2
```

- Add the N\_Port to the group using the **nport interface fibrechannel** *port* command, where *port* is a supported N\_Port number for the switch in rbridge-id/slot/port format.

```
switch(config-rbridge-id-3-ag-pg-2)# nport interface fibrechannel 3/0/3
```

You can add multiple N\_Ports by listing the ports separated by spaces. For example:

```
nport interface fibrechannel 3/0/3 3/0/5
```

- Verify that the ports were added or removed from the port groups using the **show ag pg rbridge-id** *rbridge-id* while in the privileged EXEC command mode.

```
show ag pg rbridge-id 3
```

Refer to [Displaying port grouping information](#) on page 206 for details on this command.

## Port Grouping policy modes

Port Grouping policy modes help manage VF\_Port and N\_Port operation when ports go offline or when all N\_Ports in a group are not connected to the same FC fabric.

There are two Port Grouping policy modes that you can enable using Network OS commands:

- Login Balancing (LB) is enabled by default when you create a port group.
- Modified Managed Fabric Name Monitoring (M-MFNM) mode is enabled with LB mode. You cannot disable MFNM mode for a port group unless you disable LB mode.

## Automatic Login Balancing mode

Automatic Login Balancing (LB) mode works to distribute logins across all available N\_Ports in a port group. It is enabled by default when a port group is created.

Consider the following for LB mode:

- When LB mode is disabled for a port group, the same configured VF\_Port to N\_Port mapping displays for the **show running-config ag** or **show ag** commands. This is because configured and active mapping are the same.
- When LB mode is enabled for a port group, the **show ag** command displays the current, active mapping because VF\_Port to N\_Port mapping is based on the current distributed load across all N\_Ports. The **show running-config ag** command displays the configured mapping only.
- If LB mode is enabled for a port group and a new N\_Port comes online, existing logins are undisturbed. If an N\_Port is disabled, its existing logins are distributed to available ports to maintain a balanced N\_Port-to-VF\_Port ratio.
- LB can be disabled using Network OS commands. When LB mode is disabled, VF\_Ports are not shared among N\_Ports in the port group, but can only connect to N\_Ports to which they are mapped. If an N\_Port is disabled, ENodes logged into mapped VF\_Ports log out. As a best practice to ensure device login, bind the ENode to a VF\_Port and ensure that its mapped N\_Port is online.
- LB mode is disruptive.
- If an N\_Port is removed from a port group enabled for LB mode and moved to another port group, the VF\_Ports mapped to that N\_Port remain with the N\_Port.

This is not the case for port groups not enabled for LB mode. When you remove an N\_Port from one of these port groups, the VF\_Ports mapped to the N\_Port move to the default Port Group 0 along with the N\_Port. You can then move the N\_Port to another group, but would need to re-map any VF\_Ports to the N\_Port.

- If an N\_Port is in a port group and then Automatic Login Balancing is enabled, the VF\_Ports mapped to the N\_Port are distributed among online N\_Ports in the same port group.
- You can disable or enable LB mode using the **no modes lb** or **modes lb** commands while in the port group configuration mode. Refer to [Enabling and disabling Login Balancing mode](#) on page 210.

## Enabling and disabling Login Balancing mode

Although Login Balancing (LB) mode is enabled by default when you create a port group, you can disable and enable it using Network OS CLI commands.

Access Gateway and the PG policy must be enabled for the **no modes LB** or **modes lb** commands to succeed.

Enable or disable LB mode using the **no modes LB** or **modes lb** commands while in the port group's configuration mode.

1. Enter the **configure terminal** command to enter global configuration mode.

```
switch# configure terminal
```

2. Enter the **rbridge-id id** command to enter RBridge ID configuration mode for the specific switch.

```
switch(config)# rbridge-id 3
```

3. Enter the **ag** command to enter Access Gateway configuration mode.

```
switch(config-rbridge-id-3)# ag
```

4. Enter the port group ID, such as pg 8, to enter configuration mode for the port group.

```
switch(config-rbridge-id-3-ag)# pg 8
```

5. Perform one of the following steps:

- To enable LB mode, enter **modes mode\_name**.

```
switch(config-rbridge-id-3-ag-pg-8)# modes lb
```

- To disable LB mode, enter **no modes mode\_name**.

```
switch(config-rbridge-id-3-ag-pg-8)# no modes lb
```

## Modified Managed Fabric Name Monitoring mode

Modified Managed Fabric Name Monitoring (M-MFNM) mode prevents connections from the AG VDX switch to multiple SANs to ensure that all N\_Ports in a port group connect to the same FC fabric.

Modified Managed Fabric Name Monitoring (M-MFNM) mode is enabled with LB mode. It queries the FC fabric name for a default time out value of 120 seconds. If it detects an inconsistency, for example all the N\_Ports within a port group are not physically connected to the same physical or virtual FC fabric, the following occurs:

- N\_Ports are disabled to the fabric with the lower number of connected N\_Ports.
- If more than one fabric has the same or the maximum number of ports connected, N\_Ports are disabled to the fabric with the higher "fabric names" (WWN of the Principal Switch). Ports connected to the lowest "fabric name" stay online.

Consider the following about M-MFNM mode:

- M-MFNM mode is enabled by default when you enable LB mode. You cannot disable it unless you disable LB mode.
- You can change the default time out value (tov) for fabric name queries using the **timeout fnm value** when in ag configuration mode. Refer to [Setting and displaying the fabric name monitoring TOV](#) on page 211.

## Setting and displaying the fabric name monitoring TOV

You can set the time out value (TOV) for M-MFNM queries of the fabric name to detect whether all N\_Ports in a port group are physically connected to the same physical or virtual fabric.

Access Gateway and the PG policy must be enabled for the **timeout fnm** command to succeed.

Use the **timeout fnm value** command while in ag configuration mode to set time-out value (TOV) for M-MFNM queries of the fabric name. The valid range is 30 to 3600 seconds. The default value is 120 seconds.

1. Enter the **configure** command to access global configuration mode.

```
switch# configure
```

2. Enter the **rbridge-id id** command to enter RBridge ID configuration mode for the specific switch.

```
switch(config)# rbridge-id 3
```

3. Enter the **ag** command to enter Access Gateway configuration mode.

```
switch(config-rbridge-id-3)# ag
```

4. Enter the **timeout fnm value** command to change the time out value for fabric name queries.

```
switch(config-rbridge-id-3-ag)# timeout fnm 60
```

5. Enter timeout **timeout fnm** without a value to display the current M-MFNM timeout value.

```
switch(config-rbridge-id-3-ag)# timeout fnm
() (60)
```

## Trunking in Access Gateway mode

The hardware-based Port Trunking feature enhances management, performance, and reliability of Access Gateway N\_Ports connected to Brocade fabrics.

Trunking in Access Gateway (AG) mode creates trunk groups between N\_Ports on the AG module and F\_Ports on the Edge-switch module. AG trunking configuration is mostly on the Edge switch. Note the following for trunking under Access Gateway:

- On Access Gateway ports, trunking is enabled by default.
- You can create trunk groups of up to eight ports.
- All of the N\_Ports in a trunk group should belong to the same AG-module port group.
- All of the F\_Ports in a trunk group should belong to the same Edge-switch port group.
- The maximum number of trunks supported within a port group is two.
- On the AG module, ensure consistent speed settings and connector-group settings on all of the ports within each trunk.
- On the End-switch, ensure consistent speed settings and connector-group settings on all of the ports within each trunk.
- Round-robin assignment of VF\_Ports to N\_Ports affects the actual number of N\_Ports in a trunk.

## Setting up trunking for Access Gateway

Use the following steps to set up trunking under Access Gateway.

Make sure that all of the conditions specified under "Trunking in Access Gateway mode" are fulfilled. For Edge-switch implementation details, refer to the "Trunking in Access Gateway mode" chapter in the *Fabric OS Access Gateway Administrator's Guide*.

1. On the AG-mode switch, in privileged EXEC mode, enter the **configure** command to change to global configuration mode.
2. Enter the **interface FibreChannel** *rbridge-id/slot/port* command for each port that you are adding to the trunk.

A configuration submode prompt appears.

3. Enter the **trunk-enable** command.

The following example configures the link attached to port 4 on RBridge 8 to be part of a trunk group.

```
switch# configure
Entering configuration mode terminal
switch(config)# rbridge-id 8
switch(config-rbridge-id-8)# interface FibreChannel 8/0/4
switch(config-FibreChannel-8/0/4)# trunk-enable
```

4. Toggle the AG-mode port.

```
switch(config-FibreChannel-8/0/4)# shutdown
switch(config-FibreChannel-8/0/4)# no shutdown
```

5. Toggle the Edge-switch port.  
Port trunking is now in effect between the specified ports.

### NOTE

If you move trunk-group ports out of their common port group, the trunk slave ports will be disabled. If this happens, recover by entering **shutdown** and then **no shutdown** for each disabled port.

## Access Gateway under FlexPort

FlexPort functionality enables specific ports to be dynamically reconfigured as either Fibre Channel (FC) or Ethernet ports, in several modes and speeds. This section deals with Access Gateway (AG) under FlexPort.

### NOTE

For details of FlexPort implementation, refer to "Configuring FlexPort," in the *Network OS Layer 2 Switching Configuration Guide*.

### NOTE

Forward Error Correction (FEC) is not supported in Access Gateway under FlexPort.

## Configuring Access Gateway under FlexPort

This procedure describes the recommended flow for configuring Access Gateway under FlexPort.

1. Using FlexPort commands, convert needed Ethernet ports to FC ports.  
For details, refer to "Configuring FlexPort," in the *Network OS Layer 2 Switching Configuration Guide*.
2. Configure FCoE.  
For details, refer to the "FCoE interface configuration" section of the *Network OS Layer 2 Switching Configuration Guide*.

### 3. Enable Access Gateway.

```
device# configure terminal
device(config)# rbridge-id 1
device(config-rbridge-id-1)# ag
device(config-rbridge-id-1-ag)# enable
```

The VF\_Ports are distributed evenly across all available N\_Ports.

#### NOTE

First configuring FCoE and then using FlexPort to reconfigure Ethernet ports as FC ports might lead to suboptimal login balance among online N\_Ports. If needed, refer to "Restoring\_Port login balance." You can also turn off login balancing for a Port Group (as described in "Enabling and disabling Login Balancing mode") and manually map VF\_Ports to N\_Ports.

## Restoring N\_Port login balance

If login distribution among online N\_Ports becomes uneven, use the **clear fcoe login** command to redistribute the logins.

#### NOTE

The following configurations may cause uneven login distribution:

- Access Gateway under FlexPort (following the initial setup)—Conversion of additional Ethernet ports to FC ports
- Toggle of N\_Ports—If associated VF\_Ports log in to another N\_Port and remain there

1. To view the list of logged-in devices, enter the **show fcoe login** command.

```
switch# show fcoe login
```

2. To log out the current device and log in to the least-loaded N\_Port, enter the **clear fcoe login device** command.

```
switch# clear fcoe login device 10:00:00:05:1e:8e:be:40
```

## N\_Port monitoring for unreliable links

N\_Port monitoring monitors links between N\_Ports on the switch configured in Access Gateway mode and F\_Ports on the connected FC fabric. When links are considered unreliable, the N\_Port is disabled.

Links from all N\_Ports are monitored for the number of online and offline static change notifications (SCNs) that occur during a five-minute period. If the number of SCNs on a link exceeds a set threshold, the link is considered unreliable, and the port is taken offline. VF\_Ports mapped to the N\_Port also go offline. Once the number of SCNs drops below the set threshold, the port is deemed reliable again and the N\_Port and the mapped VF\_Ports go back online.

The default threshold is 25 SCNs per 5 minutes. You can set from 10 to 100 SCNs per 5 minutes. While in **ag** command mode, you can use the **counter reliability value** command to modify the default threshold.

## Setting and displaying the reliability counter for N\_Port monitoring

You can set the reliability count of static change notifications (SCNs) counted during a five-minute period before the link between a N\_Port on a Switch in Access Gateway mode and an F\_Port on a FC fabric is considered unreliable.

Access Gateway mode must be enabled for this procedure to succeed.

To set the reliability count, use the **counter reliability value** command while in **ag** configuration mode for the switch. The default value is 25 SCNs per 5 minutes. You can set from 10 to 100 SCNs per 5 minutes.

1. Enter the **configure terminal** command to enter global configuration mode.

```
switch# configure terminal
```

2. Enter the **rbridge-id id** command to enter RBridge ID mode for the specific switch.

```
switch(config)# rbridge-id 2
```

3. Enter the **ag** command to enter Access Gateway configuration mode.

```
switch(config-rbridge-id-2)# ag
```

4. Enter the **counter reliability value** command to change the counter value.

```
switch(config-rbridge-id-2-ag)# counter reliability 50
```

5. Enter the **counter reliability** command without a value to display the current reliability counter. In the following example, a counter value of 50 is returned.

```
switch(config-rbridge-id-2-ag)# counter reliability
() (50)
```

## Displaying Access Gateway N\_Port utilization data

Under Access Gateway, the **show ag nport-utilization** command displays N\_Port utilization information. You can display this information either for a specific RBridge or for all the RBridges.

The information displayed indicates the highest bandwidth utilization and associated time stamp. Two actions clear such data:

- Enabling the port
- Running **clear ag nport-utilization**

### NOTE

For trunk slave ports, no utilization information is printed. Instead, the bandwidth of such ports is included in the bandwidth of the trunk master port.

In Privileged EXEC mode, enter **show ag nport-utilization**.

```
switch# show ag nport-utilization
```

Data such as the following displays:

```
N_Port(Fi) information :
Port          PortID          Attached PWWN          IP_Addr          VF_Ports
-----
Fi 1/0/7      0xa90900 2f:00:00:05:1e:80:31:4f 10.17.31.169    1/1/1, 1/1/2
highest bandwidth utilization of 11 % recorded at Wed Apr 30 14:07:42 2014

Fi 1/0/8      0xa90900 2f:00:00:05:1e:80:31:4f 10.17.31.169    None
trunk slave. bandwidth/traffic added to trunk master
```

# System Monitor and Threshold Monitor

---

- [System Monitor overview.....](#) 215
- [Configuring System Monitor.....](#) 216
- [Threshold Monitor overview.....](#) 218
- [Configuring Threshold Monitor.....](#) 222

## System Monitor overview

System Monitor provides customizable monitoring thresholds, which allow you to monitor the health of each component of a switch. Whenever a switch component exceeds a configured threshold, System Monitor automatically provides notification by means of e-mail or RASLog messages, depending on the configuration.

Because of platform-specific values that vary from platform to platform, it was previously not possible to configure platform-specific thresholds through a global CLI command. In Network OS 4.0.0 and later, it is possible to monitor individual switches in a logical chassis cluster or fabric cluster. This is done in RBridge ID configuration mode, by addressing the RBridge ID of the selected switch.

Threshold and notification configuration procedures are described in the following sections.

## Monitored components

The following FRUs and temperature sensors are monitored on supported switches:

- **LineCard** —Displays the threshold for the line card.
- **MM** —Displays the threshold for the management module.
- **SFM** —Displays the threshold for the switch fabric module device.
- **cid-card** —Displays the threshold for the chassis ID card component.
- **compact-flash** —Displays the threshold for the compact flash device.
- **fan** —Configures fan settings.
- **power** —Configures power supply settings.
- **sfp** —Displays the threshold for the small form-factor pluggable (SFP) device.
- **temp**—Displays the threshold for the temperature sensor component.

### NOTE

CID cards can be faulted and removed. The system continues to operate normally as long as one CID card is installed. If both CID cards are missing or faulted, the switch will not operate.

## Monitored FRUs

System Monitor monitors the absolute state of the following FRUs:

- Fan
- Power supply
- CID card
- SFP
- Line card

Possible states for all monitored FRUs are removed, inserted, on, off, and faulty. A state of none indicates the switch is not configured. If the FRU is removed, inserted, or goes into a faulty state, System Monitor sends a RASLog message or an e-mail alert, depending on the configuration.

Based on the configured threshold, each component can be in a marginal state or a down state. If a component is in a marginal state or a down state, System Monitor generates a RASLog message to alert the user. It also generates a separate RASLog message for the overall health of the switch.

#### NOTE

For details about each RASLog message, refer to the "RAS System Messages" chapter of the *Network OS Message Reference*.

The following table lists the marginal and down thresholds for components monitored by System Monitor on supported switches.

**TABLE 33** Hardware platform marginal and threshold settings for supported switches

Platform	Hardware component	Marginal threshold	Down threshold
Brocade VDX 6740	Power supply	1	2
	Temperature sensor	1	2
	Compact flash	1	0
	Fan	1	2
Brocade VDX 8770-4	Power supply	1	2
	Temperature sensor	1	2
	Compact flash	1	0
	Fan	1	2
Brocade VDX 8770-8	Power supply	6	7
	Temperature sensor	1	2
	Compact flash	1	0
	Fan	1	2

## Configuring System Monitor

This section contains example basic configurations that illustrate various functions of the **system-monitor** command and related commands.

#### NOTE

For command details, refer to the *Network OS Command Reference*.

## Setting system thresholds

Each component can be in one of two states, down or marginal, based on factory-defined or user-configured thresholds. (The default thresholds are listed in [Configuring System Monitor](#) on page 216.)

1. Issue the **configure terminal** command to enter global configuration mode.
2. Enter RBridge ID configuration mode, as in the following example.

```
switch(config)# rbridge-id 154
```

3. Change **down-threshold** and **marginal-threshold** values for the SFM.

```
switch(config-rbridge-id-154)# system-monitor sfm threshold down-threshold 3 marginal-threshold 2
```



**NOTE**

You can disable the monitoring of each component by setting **down-threshold** and **marginal-threshold** values to 0 (zero).

## Setting state alerts and actions

System Monitor generates an alert when there is a change in the state from the default or defined threshold.

1. Issue the **configure terminal** command to enter global configuration mode.
2. Enter RBridge ID configuration mode (for RBridge ID 154 in this case).

```
switch(config)# rbridge-id 154
```

To enable a RASLog alert when the power supply is removed, enter the following command:

```
switch(config-rbridge-id-154)# system-monitor power alert state removed action raslog
```

**NOTE**

There are no alerts for MM, compact-flash, or temp. There are no alert actions for SFPs.

## Configuring e-mail alerts

Use the **system-monitor-mail fru** command to configure e-mail threshold alerts for FRU, SFP, interface, and security monitoring. For an e-mail alert to function correctly, you must add the IP addresses and host names to the domain name server (DNS) in addition to configuring the domain name and name servers. A single email configuration is applicable for all switches in a logical chassis cluster. For complete information on the **system-monitor-mail relay host** command, refer to the *Network OS Command Reference*.

1. Issue the **configure terminal** command to enter global configuration mode.
2. Enter the following command to enable e-mail alerts and to configure the e-mail address.

```
switch(config)# system-monitor-mail fru enable email-id
```

## Sendmail agent configuration

The following **system-monitor-mail relay host** commands allow the sendmail agent on the switch to resolve the domain name and forward all e-mail messages to a relay server.

- To create a mapping:

```
switch(config)# system-monitor-mail relay ip-address 1.2.3.4 domain-name domain_name1.brocade.com
```

- To delete the mapping:

```
switch(config)# no system-monitor-mail relay ip-address 1.2.3.4 domain-name domain_name1.brocade.com
```

- To change the domain name:

```
switch(config)# system-monitor-mail relay ip-address 1.2.3.4 domain-name domain_name2.brocade.com
```

**NOTE**

You must delete the first domain name before you can change it to a new domain name.

- To delete the domain name and return to the default:

```
switch(config)# no system-monitor-mail relay ip-address 1.2.3.4 domain-name domain_name2.brocade.com
```

## Viewing system SFP optical monitoring defaults

You can view the optical monitoring default values by entering **show defaults threshold** followed by the SFP type.

The following example command will display the defaults for type 1GLR SFPs:

```
switch# show defaults threshold sfp type 1GLR
```

## Displaying the switch health status

To display the health status of a switch, enter **show system monitor**.

```
switch# show system monitor
** System Monitor Switch Health Report **
RBridge 154      switch status      : MARGINAL
                  Time of Report      : 2013-03-24 20:51:53
                  Power supplies monitor : MARGINAL
                  Temperatures monitor  : HEALTHY
                  Fans monitor          : HEALTHY
                  Flash monitor         : HEALTHY
```

## Threshold Monitor overview

The **threshold-monitor** commands allow you to monitor CPU and memory usage of the system, interface and SFP environmental status, and security status and be alerted when configured thresholds are exceeded. These commands are configured in RBridge ID configuration mode to support fabric cluster and logical chassis cluster topologies.

In addition to the policy keywords (available for **interface**, **SFP**, and **security monitoring**), you can use the **custom** keyword create your own custom policies that have non-default thresholds, and apply them by means of the **apply** operand. This allows you to toggle between default settings and saved custom configuration settings and to apply actions and thresholds separately. For example, you can choose to use default threshold settings together with a customized subset of available actions, or you can modify some of the threshold settings and use the default action settings. You can also pause monitoring and actions by means of the **pause** keyword.

For detailed information on the variables and keywords (operands) of the **threshold-monitor** series of commands, refer to the *Network OS Command Reference*.

## CPU and memory monitoring

When configuring CPU monitoring, specify a value in the 1-100 range. When the CPU usage exceeds the limit, a threshold monitor alert is triggered. The default CPU limit is 75 percent. With respect to memory, the limit specifies a usage limit as a percentage of available resources.

When used to configure memory or CPU threshold monitoring, the limit value must be greater than the low limit and smaller than the high limit. The alert provided is a RASLog message, with the following options configurable under the **raslog** option of the **threshold-monitor cpu** or the **threshold-monitor memory** commands:

<b>high-limit</b>	Specifies an upper limit for memory usage as a percentage of available memory. This value must be greater than the value set by <b>limit</b> . When memory usage exceeds this limit, a RASLog CRITICAL message is sent. Valid values range from 0 through 80 percent.
<b>limit</b>	Specifies the baseline memory usage limit as a percentage of available resources. When this value is exceeded, a RASLog WARNING message is sent. When the usage returns below the value set by <b>limit</b> , a RASLog INFO message is sent. Valid values range from 0 through 80 percent.
<b>low-limit</b>	Specifies a lower limit for memory usage as percentage of available memory. This value must be smaller than the value set by <b>limit</b> . When memory usage exceeds or falls below this limit, a RASLog INFO message is sent.
<b>poll</b>	Specifies the polling interval in seconds. Valid values range from 0 through 3600.

**retry** Specifies the number of polling retries before desired action is taken. Valid values range from 1 through 100.

#### NOTE

For CPU and memory thresholds, the low limit must be the lowest value and the high limit must be the highest value.

The table below lists the factory defaults for CPU and memory thresholds.

**TABLE 34** Default values for CPU and memory threshold monitoring

Operand	Memory	CPU
<b>low-limit</b>	40%	N/A
<b>limit</b>	60%	75%
<b>high-limit</b>	70%	N/A
<b>poll</b>	120 seconds	120 seconds
<b>retry</b>	3	3

## SFP monitoring

The SFP parameters that can be monitored are listed and described below.

**TABLE 35** SFP parameter descriptions

SFP parameter	Description	Suggested SFP impact
Temperature	Measures the temperature of the SFP, in degrees Celsius.	High temperature suggests the SFP might be damaged.
Receive power (RXP)	Measures the amount of incoming laser, in $\mu$ Watts.	Describes the condition of the SFP. If this parameter exceeds the threshold, the SFP is deteriorating.
Transmit power (TXP)	Measures the amount of outgoing laser power, in $\mu$ Watts.	Describes the condition of the SFP. If this parameter exceeds the threshold, the SFP is deteriorating.
Current	Measures the amount of current supplied to the SFP transceiver.	Indicates hardware failures.
Voltage	Measures the amount of voltage supplied to the SFP.	A value higher than the threshold indicates the SFP is deteriorating.

## SFP thresholds

You can customize SFP thresholds or actions by using the **threshold-monitor sfp** command, which enables you to perform the following tasks.

- Customize SFP configurations or accept SFP defaults.
- Manage the actions and thresholds for the Current, Voltage, RXP, TXP, and Temperature areas of the SFP.
- Suspend SFP monitoring.

If you do not provide the SFP type parameters, the default thresholds and actions are used. SFP types, monitoring areas, and default threshold values for the 16-Gbps and QSFP SFPs are detailed below.

**TABLE 36** Factory thresholds for SFP types and monitoring areas

SfpType	Area	Default Value	
1 GSR	Temperature (C)	100	-40
	Voltage (mV)	3600	3000

**TABLE 36** Factory thresholds for SFP types and monitoring areas (continued)

SfpType	Area	Default Value	
	RXP ( $\mu$ W)	1122	8
	TXP ( $\mu$ W)	1000	60
	Current (mA)	12	2
1 GLR	Temperature (C)	90	-45
	Voltage (mV)	3700	2900
	RXP ( $\mu$ W)	501	6
	TXP ( $\mu$ W)	794	71
	Current (m)	45	1
10 GSR	Temperature (C)	90	-5
	Voltage (mVolt)	3600	3000
	RXP ( $\mu$ W)	1000	32
	TXP ( $\mu$ W)	794	251
	Current (mA)	11	4
10 GLR	Temperature (C)	88	-5
	Voltage (mV)	3600	2970
	RXP ( $\mu$ W)	1995	16
	TXP ( $\mu$ W)	1585	158
	Current (mA)	85	15
10 GUSR	Temperature (C)	100	-5
	Voltage (mV)	3600	2970
	RXP ( $\mu$ W)	2000	32
	TXP ( $\mu$ W)	2000	126
	Current (mA)	11	3
QSFP	Temperature (C)	75	-5
	Voltage (mV)	3600	2970
	RXP ( $\mu$ W)	1995	40
	TXP ( $\mu$ W)	0	0
	Current (mA)	10	1

## Threshold values

High and low threshold values are the values at which potential problems might occur. For example, in configuring a temperature threshold for SFPs, you can select the temperatures at which a potential problem can occur because of overheating or overcooling.

A combination of high and low threshold settings can cause the following actions to occur:

- Above high threshold — A default or user-configurable action is taken when the current value is above the high threshold.
- Below high threshold — A default or user-configurable action is taken when the current value is between the high and low threshold.
- Below low threshold — A default or user-configurable action is taken when the current value is below the low threshold.
- Above low threshold — monitoring is not supported for this value.

## Security monitoring

You can monitor all attempts to breach your SAN security, helping you fine-tune your security measures. If there is a security breach, you can configure an email or RASLog alert to be sent. The following security areas are monitored:

- Telnet Violation, which occurs when a Telnet connection request reaches a secure switch from an unauthorized IP address.
- Login Violation, which occurs when a secure fabric detects a login failure.

The following table lists the factory defaults for security area settings.

**TABLE 37** Security area default settings

Area	High threshold	Low threshold	Buffer	Timebase
Telnet Violation	2	1	0	Minute
Login Violation	2	1	0	Minute

## Interface monitoring

You can set thresholds for error statistics on all external Gigabit Ethernet interfaces. When any monitored error crosses the configured high or low threshold, an alert can be generated or a problem interface can be isolated (refer to [Port Fencing](#) on page 222).

### Interface error types

The following table describes the interface counters that can be monitored on external interfaces.

**TABLE 38** Interface errors that can be monitored on external interfaces

Interface area	Description	Port Fencing support	Threshold defaults
MissingTerminationCharacter	Number of frames terminated by anything other than the Terminate character; this includes termination due to the Error character.	No	Low 12 Buffer 0 High 300
CRCAlignErrors	Total number of frames received that had a length (excluding framing bits but including Frame Check Sequence (FCS) octets) of between 64 and 1518 octets. The error indicates either a bad FCS with an integral number of octets (an FCS error) or a bad FCS with a non-integral number of octets (an alignment error).	No	Low 12 Buffer 0 High 300
IFG	Minimum-length interframe gap (IFG) between successive frames is violated. A typical IFG is 12 bytes.	Yes	Low 5 Buffer 0 High 100
SymbolErrors	An undefined (invalid) symbol received on the interface. Large symbol errors indicate a bad device, cable, or hardware.	No	Low 0 Buffer 0 High 5

#### NOTE

The default setting for above high threshold, above low threshold, below high threshold, and below low threshold actions is "[none]."

## Port Fencing

A port that is consistently unstable can harm the responsiveness and stability of the entire fabric and diminish the ability of the management platform to control and monitor the switches within the fabric. *Port Fencing* is not enabled by default; it disables the interface if a user-defined high threshold is exceeded. When a port that has exceeded its user-defined high threshold is fenced by software, the port is placed in the "Disabled" state and held offline. After a port is disabled, user intervention is required for frame traffic to resume on the port.

### NOTE

*Port Fencing* is supported for the "RX IFG Violated" error only.

## Configuring Threshold Monitor

The following basic configurations illustrate various functions of the **threshold-monitor** commands.

### NOTE

For CLI details, refer to the *Network OS Command Reference*

## Viewing threshold status

To view the status of currently configured thresholds, enter the **show running-config threshold-monitor** command with the RBridge ID, as follows:

```
switch# show running-config rbridge-id rbridge_id threshold-monitor
```

### NOTE

Default values are not displayed under the **show running-config threshold-monitor** command. Only custom values are displayed when a user applies a policy.

To display the default values of thresholds and alert options, enter the **show defaults threshold** command, as in the following example for interfaces.

```
switch# show defaults threshold interface type Ethernet

Type: GigE-Port
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|          | High Threshold |          |          | Low Threshold | Buffer | Time | | |
| Area    | Value  | Above | Below | Value  | Above | Below | Value | Base |
|          |         | Action| Action|         | Action| Action|       |      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|MTC     | 300   | none  | none  | 12    | none  | none  | 0     | minute |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|CRCAlign| 300   | none  | none  | 12    | none  | none  | 0     | minute |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|Symbol  | 5     | none  | none  | 0     | none  | none  | 0     | minute |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|IFG     | 100  | none  | none  | 5     | none  | none  | 0     | minute |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
MTC - Missing Termination Character
```

## CPU and memory threshold monitoring

### NOTE

Support for the custom **policy** operand is not provided for CPU and memory threshold monitoring.

## Configuring CPU monitoring thresholds and alerts

CPU monitoring allows you to set alerts for CPU usage.

1. Enter **configure terminal** to enter global configuration mode.

```
switch# configure terminal
switch(config)#
```

2. Enter **rbridge-id rbridge-id#** to change to RBridge ID configuration mode.

```
switch(config)# rbridge-id 154
switch(config-rbridge-id-154)#
```

3. Enter **threshold-monitor cpu ?** to view the available options:

```
switch(config-rbridge-id-154)# threshold-monitor cpu ?
```

The following example changes the thresholds from the default, adjusts polling and retry attempts, and causes a RASLog message to be sent when thresholds are exceeded.

```
switch(config-rbridge-id-154)# threshold-monitor cpu actions raslog limit 65 poll 60 retry 10
```

### NOTE

This command does not support **low-limit** or **high-limit** under the **raslog** alert option.

## Configuring memory monitoring thresholds and alerts

CPU monitoring allows you to set alerts for memory usage.

1. Enter **configure terminal** to enter global configuration mode.

```
switch# configure terminal
switch(config)#
```

2. Enter **rbridge-id rbridge-id#** to change to RBridge ID configuration mode.

```
switch(config)# rbridge-id 154
switch(config-rbridge-id-154)#
```

3. Enter **threshold-monitor memory ?** to view the available options.

```
switch(config-rbridge-id-154)# threshold-monitor memory ?
```

The following example changes the thresholds from the default and causes no message to be sent when thresholds are exceeded.

```
switch(config-rbridge-id-1)# threshold-monitor memory actions none high-limit 60 low-limit 40
```

## Configuring SFP monitoring thresholds and alerts

The following is an example of configuring SFP monitoring.

1. Enter **configure terminal** to enter global configuration mode.

```
switch# configure terminal
switch(config)#
```

2. Enter **rbridge-id rbridge-id#** to change to RBridge ID configuration mode.

```
switch(config)# rbridge-id 154
switch(config-rbridge-id-154)#
```

3. Enter **threshold-monitor sfp** and create a custom policy.

```
switch(config-rbridge-id-154)# threshold-monitor sfp policy mypolicy type lglr area temperature
alert above highthresh-action raslog email
```

#### NOTE

Refer also to [Security monitoring](#) on page 221 for more information.

4. Apply the policy.

```
switch(config-rbridge-id-154)# threshold-monitor sfp apply mypolicy
```

## Security monitoring

Security monitoring allows you to set security threshold and alert options, including login-violation or telnet-violation alerts.

### Viewing security defaults

To display the default values of security threshold and alert options, enter the **show defaults security area** command with the **login-violation** or **telnet-violation** options.

```
switch# show defaults security area login-violation
```

### Configuring security monitoring

1. Issue the **configure terminal** command to enter global configuration mode.
2. Enter RBridge ID configuration mode, as in the following example.

```
switch(config)# rbridge-id 154
```

3. Enter the **threshold-monitor security** command to configure custom login-violation monitoring, as in the following example.

```
switch(config-rbridge-id-154)# threshold-monitor security
policy mypolicy area login-violation alert above highthresh-action
raslog below highthresh-action email lowthresh-action none
```

4. Apply the policy.

```
switch(config-rbridge-id-154)# threshold-monitor security apply mypolicy
```

## Configuring Interface monitoring

The following sections discuss how to view interface threshold defaults and configure interface monitoring.

### Viewing interface threshold defaults

Use the following command to view interface threshold defaults.

```
switch# show defaults threshold interface type Ethernet
```

Refer to [Viewing threshold status](#) on page 222 for the results of this command.

### Configuring interface monitoring

1. Issue the **configure terminal** command to enter global configuration mode.



2. Enter RBridge ID configuration mode (in this case, for RBridge ID 154).

```
switch(config)# rbridge-id 154
```

3. Enter the **threshold-monitor interface** command to configure custom interface monitoring, as in the following example.

```
switch(config-rbridge-id-154)# threshold-monitor interface policy mypolicy type ethernet area  
missingterminationcharacter alert above lowthresh-action email
```

4. Apply the policy.

```
switch(config-rbridge-id-154)# threshold-monitor interface apply mypolicy
```

## Pausing and continuing threshold monitoring

By default, threshold monitoring is enabled.

To disable monitoring of a particular type, enter the **threshold-monitor [cpu | interface | memory | security | sfp] pause** command.

To re-enable monitoring, enter the **no** of the **threshold-monitor** command.

### NOTE

Not all functions of the **threshold-monitor** command can be disabled. Continue to enter **?** at each level of the command synopsis to confirm which functions can be disabled.



# VMware vCenter

---

- [vCenter and Network OS integration overview](#)..... 227
- [vCenter discovery](#)..... 228
- [vCenter configuration](#)..... 228

## vCenter and Network OS integration overview

The VMware vCenter Server allows for the management of multiple ESX /ESXi servers and virtual machines (VMs) from different ESX servers through a single graphical user interface (GUI). It provides unified management of all the hosts and VMs in the data center, from a single console with an aggregate performance monitoring of clusters, hosts and VMs.

The VMware vCenter and Brocade Network OS integration supported in Brocade VCS Fabric mode enables you to discover VMware ESX servers managed by a vCenter server. VMware's server hosts (ESX servers) are connected directly to the physical switches through the switch ports (edge ports in Brocade VCS Fabric mode). The server hosts implement a virtual switch (vSwitch), which is used to provide connections to the VMs. The fundamental requirement for the vCenter and Network OS integration is the IP-level management connectivity of the vCenter Server 4.0 version and later with the Brocade VDX switches.

### NOTE

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

You can view virtual switches and virtual machines, their associated MAC addresses, and network policies using the Network OS command line interface (CLI). Refer to the *Network OS Command Reference* for details about the **vcenter** and **vnetwork** commands.

## vCenter properties

The vCenter manages the VMware ESX/ESXi hosts. The vCenter user interface is provided through a vSphere client on the same management network as the vCenter, and virtual machines (VMs) are created using the vSphere client user interface. In addition to creating the VMs, the server administrator associates the VMs with distributed virtual switches, distributed virtual port groups, standard virtual switches (vSwitches) and standard port groups.

The vCenter automatically generates some of the VM properties (such as the MAC address), and some properties must be configured (such as the VLAN properties). Most of the VM configuration, including network policies, is done using the vCenter's vSphere user interface and is beyond the scope of this document.

For VMWare configuration information, visit the VMware documentation site.

## vCenter guidelines and restrictions

Follow these guidelines and restrictions when configuring vCenter:

- Special characters in the port group names are replaced with the URL-encoded values.
- Standard port groups with the same name that reside in different ESX/ESXi hosts must have identical VLAN settings across all hosts.
- For all vCenter port groups, Network OS automatically creates a port profile with the following format: `auto-vcenter_name-datacenter_ID-port-group-name`. User editing of these auto port groups is not supported.
- Network OS supports vCenter discovery that is based on events.
- Network OS supports LLDP and QoS (IEEE 8021p) for distributed virtual switches (dvSwitches).
- Using port-profile names fewer than 63 characters has been shown to conserve CPU resources.

- CDP/LLDP-receiving interface ports must not have any conflicting configurations on the interface that prevent them from being in a port-profiled mode.
- An interface is prevented from becoming a port-profile-port only when conflicting switchport, QoS, and security configurations reside on the interface. An FCoE configuration on the interface does not prevent a port-profile-port configuration.
- Before configuring a vCenter in the fabric, remove all the manually created port profiles that have vCenter inventory MAC associations.
- Up to four vCenter configurations are supported per fabric, with support for multiple data centers.
- Duplicate vCenter asset values are not supported, such as duplicate MAC addresses and duplicate Host names.

#### NOTE

Refer to the *Release Notes* for the number of port groups supported per platform, as well as other related information.

## vCenter discovery

A Brocade VDX switch connected to VMware ESX/ESXi hosts and virtual machines must be aware of network policies in order to allow or disallow traffic; this requires a discovery process by the VDX switch. During VDX switch configuration, relevant vCenters that exist in its environment and the discovery of virtual assets from the vCenter occurs in the following circumstances:

- When a switch boots up
- When a new vCenter is configured on the VDX switch and activated (activation turns on the timer processing, set to 30-minute intervals)
- When the discovery is explicitly initiated with the CLI

The following assets are discovered from the vCenter:

- Hosts and data centers associated with the vCenter
- Virtual machines (VMs) that have been created on the hosts
- VMware distributed virtual port groups (dvPortGroups)
- Standard port groups, with QoS priority associated with a dvPortGroup
- Standard virtual switches
- Distributed virtual switches

## vCenter configuration

Configuring vCenter consists of three basic steps performed in this order:

1. Enabling VMware vSphere QoS.
2. Enabling CDP/LLDP on switches.
3. Adding and activating the vCenter.

These steps and postconfiguration steps are discussed in this section.

### Step 1: Enabling QoS

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

## Step 2: Enabling CDP/LLDP

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

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

### Enabling CDP/LLDP on vSwitches

Complete the following steps to enable CDP/LLDP on virtual switches (vSwitches).

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

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

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

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

### Enabling CDP/LLDP on dvSwitches

Complete the following steps to enable CDP on distributed virtual switches (dvSwitches).

1. Connect to the vCenter server by using the vSphere Client.
2. On the vCenter Server home page, click **Networking**.
3. Right-click the distributed virtual switches (dvSwitches) and click **Edit Settings**.
4. Select **Advanced** under **Properties**.
5. Use the check box and the drop-down list to change the CDP/LLDP settings.

## Step 3: Adding and activating the vCenter

After CDP is enabled on all the vSwitches and dvSwitches in the vCenter, configuration on the Network OS side is a two-step process, consisting of adding the vCenter and activating the vCenter.

### Adding the vCenter

You must add the vCenter before initiating any discovery transactions. To authenticate with a specific vCenter, you must first configure the URL, login, and password properties on the VDX switch.

#### NOTE

By default, the vCenter server accepts only HTTPS connection requests.

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

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

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

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

## Activating the vCenter

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

### NOTE

In VCS mode, you can configure the vCenter by using any node. Discovery is initiated by the primary node.

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

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

Immediately following first-time vCenter activation, the Network OS starts the virtual asset discovery process. Use the **show vnetwork vcenter status** command to display the vnetwork status, as in the following example.

```
switch# show vnetwork vcenter status
vCenter          Start                Elapsed (sec)      Status
=====          =====
myvcenter        2011-09-07 14:08:42  10                 In progress
```

When the discovery process completes, the status displays as "Success." Network OS has performed all the necessary configurations needed for the vCenter Server, and is now ready for CDP transmissions from the virtual switches to identify which ESX/ESXi host is connected to which physical interface in the Ethernet Fabric.

## Discovery timer interval

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

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

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

### NOTE

Best practice is to keep the discovery timer interval value at the default (30). A value of 0 disables the periodic vCenter discovery.

## User-triggered vCenter discovery

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

- When a switch boots up.
- When a new vCenter is configured on the VDX switch and activated (activation turns on the timer processing, set to 180-second intervals.)
- When the discovery is explicitly initiated with the CLI.

To explicitly initiate vCenter discovery, perform the following task in global configuration mode.

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

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

- Return to privileged EXEC mode with the **exit** command.

```
switch(config)# exit
switch#
```

- Use the **vnetwork vcenter** command to trigger a vCenter discovery manually.

```
switch# vnetwork vcenter myvcenter discover
```

## Viewing the discovered virtual assets

Enter one of the following **show vnetwork** asset commands:

- show vnetwork datacenter vcenter** *vcenter\_name*

### NOTE

The **datacenter** keyword is optional in the following commands and need not be used unless required.

- show vnetwork dvpgs datacenter** *datacenter\_id* **vcenter** *vcenter\_name*
- show vnetwork dvs datacenter** *datacenter\_id* **vcenter** *vcenter\_name*
- show vnetwork hosts datacenter** *datacenter\_id* **vcenter** *vcenter\_name*
- show vnetwork pgs datacenter** *datacenter\_id* **vcenter** *vcenter\_name*
- show vnetwork vcenter status**
- show vnetwork vmpolicy macaddr datacenter** *datacenter\_id* **vcenter** *vcenter\_name*
- show vnetwork vms datacenter** *datacenter\_id* **vcenter** *vcenter\_name*
- show vnetwork vss datacenter** *datacenter\_id* **vcenter** *vcenter\_name*

where:

- dvpgs** — Displays discovered distributed virtual port groups.
- dvs** — Displays discovered distributed virtual switches.
- hosts** — Displays discovered hosts.
- pgs** — Displays discovered standard port groups.
- vcenter status** — Displays configured vCenter status.
- vmpolicy** — Displays the following network policies on the Brocade VDX switch: associated media access control (MAC) address, virtual machine, (dv) port group, and the associated port profile.
- vms** — Displays discovered virtual machines (VMs).
- vss** — Displays discovered standard virtual switches.

Refer to the *Network OS Command Reference* for detailed information about the **show vnetwork** commands.



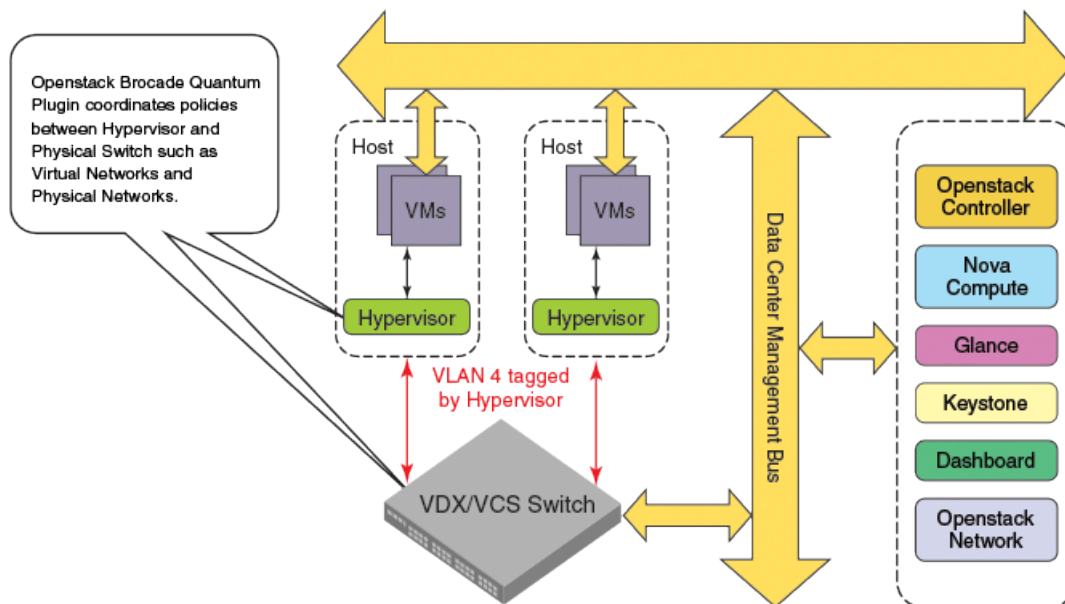


# Overview of OpenStack

OpenStack is an open-source Infrastructure as a Service (IaaS) initiative for creating and managing large groups of virtual private servers in a cloud computing environment. The Brocade Neutron ML2 Plugin for VDX/VCS provides a means to interface with OpenStack's networking to orchestrate the Brocade physical switches.

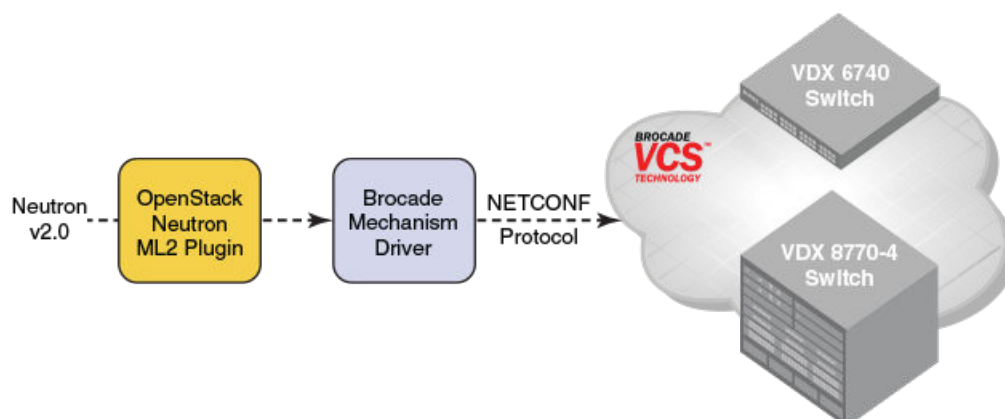
In cloud environments where virtual machines (VMs) are hosted by physical servers, the VMs see a new virtual access layer provided by the host machine. This new access layer can be created using many mechanisms, such as Linux bridges or virtual switches. The policies of the virtual access layer (virtual network) must be coordinated with the policies set in the hardware switches. The Brocade Neutron plugin helps coordinate this behavior automatically without any need for intervention by the administrator.

FIGURE 39 Virtual and physical network orchestration



The Brocade Neutron ML2 Plugin communicates with the Brocade Mechanism Driver, which uses NETCONF on the backend to configure the Brocade switches.

FIGURE 40 OpenStack configuration path



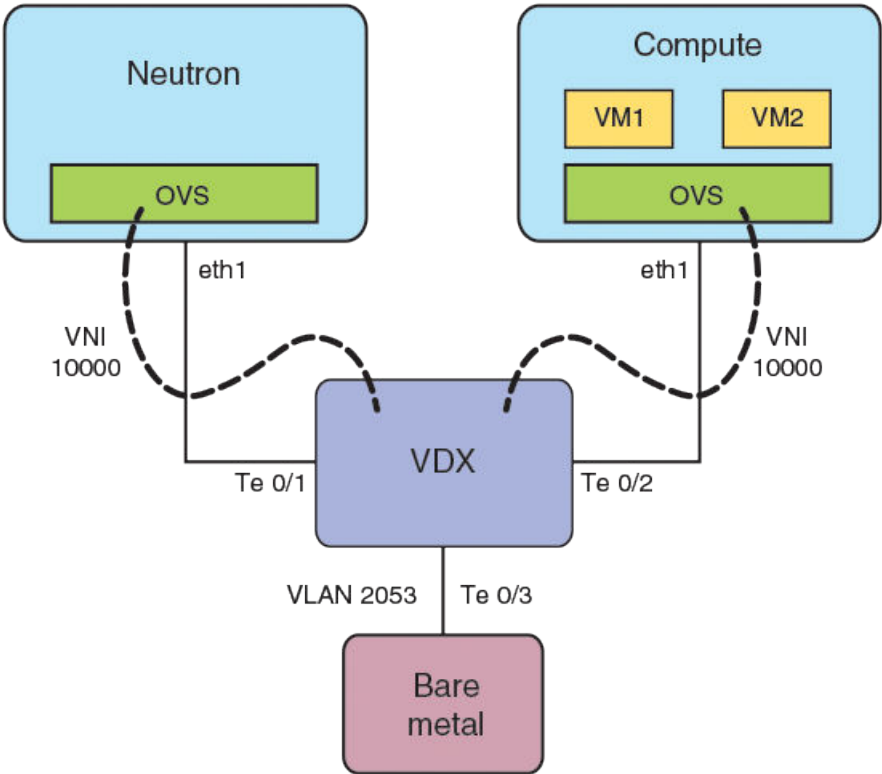
For the latest version of the OpenStack Neutron plugin, go to the <https://wiki.openstack.org/wiki/Neutron> site and search under plugins for the Brocade plugin. The OpenStack community can be contacted at <http://www.openstack.org/>.

## OpenStack L2 Gateway

Beginning with Network OS 7.0.0, support is provided for OpenStack L2 Gateway with the OpenStack "Kilo" release. OpenStack L2 Gateway is a plugin that bridges Layer 2 traffic between the virtual world (VMs in the OpenStack Compute node) and the physical world (a Brocade VDX). OpenStack uses Open vSwitch Database (OVSDB) to distribute configurations between itself and the VDX, acting as an OVSDB client while the VDX acts as an OVSDB server.

As illustrated in the following figure, the OpenStack servers are connected physically to the VDX switch. The Neutron node handles the networking construct, whereas the Compute node hosts VMs and their lifecycles. When configured (see "Configuring support for OpenStack," below), tunnels are established between the VDX and the compute nodes.

FIGURE 41 OpenStack L2 Gateway topology



----- VXLAN tunnel

**NOTE**

This configuration is similar, but not identical, to configuring a VXLAN gateway for NSX Controller deployments.



# Configuring Support for OpenStack

- [Configuring OpenStack to access Network OS.....](#) 237
- [Configuring OpenStack support for Layer 2 gateways.....](#) 237
- [Configuring OpenStack support for Layer 2 population.....](#) 238
- [Configuring a Layer 2 gateway to connect as an OpenStack SSL client.....](#) 239
- [Configuring a VDX as an OVSDB SSL server for OpenStack.....](#) 239

This section presents the configurations that Brocade currently supports for OpenStack.

## Configuring OpenStack to access Network OS

You must configure the Neutron Plugin and Brocade configuration to activate OpenStack access.

The Brocade ML2 drivers have been certified on Redhat and Ubuntu.

1. Look for the following sections in the `brocade.ini` configuration file and modify the physical switch configuration parameters and the Brocade-specific database configuration as shown below.

```
% cat /etc/neutron/plugins/brocade/brocade.ini

[SWITCH]
username = admin
password = password
address = <switch mgmt ip address>
ostype = NOS

[DATABASE]
sql_connection = mysql://root:pass@localhost/brcd_Neutron?charset=utf8
```

2. Similarly, modify the `m12_config.ini` file to enable the Brocade ML2 mechanism drivers as shown below.

```
% cat /etc/neutron/plugins/ml2/ml2_conf.ini

[m12]
tenant_network_types = vlan
type_drivers = local,flat,vlan,gre,vxlan
mechanism_drivers = openvswitch,brocade
```

3. (Optional) To enable Layer 2 gateway functionality, proceed to "Configuring OpenStack support for Layer 2 gateways" in this section for additional Neutron configurations.

## Configuring OpenStack support for Layer 2 gateways

This task sets up the OpenStack environment on the Neutron to support Layer 2 gateways.

The OpenStack version must be the "Kilo" release, which provides the L2 Gateway plugin.

1. Obtain the plugin code from GitHub and install it on the controller node by means of the following Git command.

```
% git clone https://github.com/openstack/networking-l2gw.git
```

2. Once the file is downloaded and installed, the following file must be modified:

```
% cat /etc/neutron/plugins/ml2/ml2_conf.ini
```

- Look for the following lines and edit the `ml2_conf.ini` file so that `"L2_population" = true`.

```
[agent]
L2_population=true
```

## Configuring OpenStack support for Layer 2 population

This task configures OpenStack on the Neutron server to support Layer 2 population, creating a gateway representation of a Brocade VDX in OpenStack.

This configuration consists of (1) declaring a VXLAN `network_type` and `segmentation_id`, (2) declaring the Layer 2 gateway, and (3) mapping the VXLAN network on OpenStack with the VLAN network on the Brocade VDX.

- Create a Neutron VXLAN network on the Neutron node, using the following syntax.

```
neutron net-create [-h] [-f {html,json,shell,table,value,yaml}]
                  [-c COLUMN] [--max-width <integer>]
                  [--prefix PREFIX] [--request-format {json,xml}]
                  [--tenant-id TENANT_ID] [--admin-state-down]
                  [--shared] [--router:external]
                  [--provider:network_type <network_type>]
                  [--provider:physical_network <physical_network_name>]
                  [--provider:segmentation_id <segmentation_id>]
                  [--vlan-transparent {True,False}]
                  NAME
```

"NAME" is the network name, which is "myNetwork" in the following example. The `segmentation_id` is the VXLAN Network Identifier (VNI) used by the VDX. The status of the configuration is confirmed as follows.

```
user@compute-128:~$ neutron net-list
+-----+
+-----+
| id | name |
+-----+-----+
| 28773e89-8242-480c-bae9-2671c4e89b26 | myNetwork | 350bccdb-33b2-41ff-b491-22a9ed9f2316 |
| 10.10.10.0/24 |
+-----+-----+

user@compute-128:~$ neutron net-show myNetwork
+-----+-----+
| Field | Value |
+-----+-----+
| admin_state_up | True |
| id | 28773e89-8242-480c-bae9-2671c4e89b26 |
| mtu | 0 |
| name | myNetwork |
| provider:network_type | vxlan |
| provider:physical_network | |
| provider:segmentation_id | 10000 |
| router:external | False |
| shared | False |
| status | ACTIVE |
| subnets | 350bccdb-33b2-41ff-b491-22a9ed9f2316 |
| tenant_id | 1156a7a420244196b8c95246c5c53095 |
+-----+-----+

user@compute-128:~$
```

- Define the gateway. The syntax is as follows:

```
% neutron l2-gateway-create <gateway_name> --
device_name='<switch_name>', interface_names='<port_name_with_vlan>'
```

Our example uses `gateway_name = "gw1"`, `device_name = "VCS-10"`.

and `interface_names = "<OVSDb-Port-name>|<data-vlan-to-be-exported-from-VDX>".`

```
% neutron l2-gateway-create gw1 --device name='VCS-10',interface_names='<OVSDb-Port-name>|<data-vlan-to-be-exported-from-VDX>'
```

The number "2053" is the VLAN on the VDX side.

3. Make a connection to the gateway. The syntax is as follows:

```
% neutron l2-gateway-connection-create <gateway_name> <network_name>
```

Our example associates the gateway, "GW1", with the VXLAN network, "myNetwork".

```
% neutron l2-gateway-connection-create gw1 myNetwork
```

Proceed to "Configuring a Layer 2 gateway to connect as an OpenStack SSL client".

## Configuring a Layer 2 gateway to connect as an OpenStack SSL client

This task configures a Layer 2 gateway to connect as an OpenStack SSL client, with support for certificates.

By default, a Layer 2 gateway connects as a TCP client. For a Layer 2 gateway to connect as an SSL client, the following changes are required in the controller node's configuration file to support certificates.

To set the certificate path, the user must create three directories, to support the key, the certificate, and the `ca_certificate` (the server certificate), respectively. Each directory path must be defined in the `l2gateway_agent.ini` file.

1. In `/etc/neutron/l2gateway_agent.ini`, edit the variables below to support the installation.

```
l2_gw_agent_priv_key_base_path = '<private key file path>'
l2_gw_agent_cert_base_path = '<certificate file path>'
l2_gw_agent_ca_cert_base_path = '<ca_certificate file path>'
```

The certificate must be copied to the `'<certificate file path>'` mentioned in the `l2gateway_agent.ini` file on the controller node.

2. Generate the certificate on the VDX (see "Configuring an OVSDb SSL server for OpenStack"), then manually copy and paste the certificate on the controller node.

### NOTE

The certificate must be copied to the `<ca_certificate file path>`. This must be done before the server is started.

Proceed to "Configuring a VDX as an OVSDb SSL server for OpenStack."

## Configuring a VDX as an OVSDb SSL server for OpenStack

This task configures a Brocade VDX as an SSL server to support the connection request from OpenStack.

The VLAN (2053) that is mapped to the VNI (10000) must be defined.

1. Do the following to specify an overlay gateway and type, attach the appropriate VLAN, specify a server name and port, enable certificate generation, and activate the server.
  - a) Enter global configuration mode, then enter the `overlay-gateway name type hardware-vtep` command.

**NOTE**

The **type hardware-vtep** keywords are required to specify that this deployment supports OpenStack deployments.

```
device# config
device(config)# overlay-gateway mygateway
device(config-overlay-gw-mygateway)# type hardware-vtep
device(config-overlay-gw-mygateway)#
```

- b) Enter the **attach rbridge-id** command to attach existing RBridge IDs to this VXLAN gateway instance. You can specify a range of RBridge IDs up to a maximum of four.

```
device(config-overlay-gw-mygateway)# attach rbridge-id add 2
device(config-overlay-gw-mygateway)#
```

- c) Attach the VLAN.

```
device(config-overlay-gw-mygateway)# attach vlan 2053
```

- d) Enter the **ip interface ve veid vrrp-extended-group group-ID** command to set the IP address of the VXLAN overlay gateway, as shown in the following example.

```
device(config-overlay-gw-mygateway)# ip interface ve 11 vrrp-extended-group
106
device(config-overlay-gw-mygateway)#
```

The command accepts the VE interface ID and VRRP-E group ID, then sets the VXLAN overlay gateway's IP address as identical to the already configured VRRP-E virtual IP address. Tunnels that form use this IP address as the source IP address for outgoing packets.

- e) Enter the **activate** command to activate this gateway instance.

```
device(config-overlay-gw-gateway1)# activate
device(config-overlay-gw-gateway1)#
```

This creates the local VTEP and enables all tunnels associated with this gateway. (VXLAN tunnels are not user configurable.)

- f) Return to privileged EXEC mode.

```
device(config-overlay-gw-gateway1)# end
device(config)# end
device#
```

2. In privileged EXEC mode, generate the security certificate for the VXLAN overlay gateway by entering the **nsx-controller client-cert generate** command.

**NOTE**

Certificate generation is a one-time-only action.

```
device# nsx-controller client-cert generate
```

3. In privileged EXEC mode, you can display the certificate by entering the **show nsx-controller client-cert** command, then provide the certificate to the administrator.

The CLI is the same as for certificate generation. Although the Cli includes **nsx** keyword, the generated certificate can be used with both OpenStack and NSX, as both require SSL certificates.

4. Specify an Open vSwitch Database (OVSDB) SSL server and configure it.



- a) In global configuration mode, use the **ovsdb-server** command to specify a server and enter OVSDB server configuration mode.

```
device# config terminal
device(config)# ovsdb-server myserver
device(config-ovsdb-server-myserver)#
```

- b) (Optional). Use the **port** command to configure a nondefault port for connection to the server. (The default is 6640).

```
device(config-ovsdb-server-myserver)# port 6641
```

- c) Use the **activate** command to activate the server.

```
device(config-ovsdb-server-myserver)# activate
```

- d) Use the **show running-config ovsdb-server** and **show ovsdb-server** commands to confirm the configuration.



# Remote Monitoring

---

- [RMON overview](#)..... 243
- [Configuring and managing RMON](#)..... 243

## RMON overview

Remote monitoring (RMON) is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

## Configuring and managing RMON

Both alarms and events are configurable RMON parameters.

- Alarms allow you to monitor a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms are paired with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Events determine the action to take when an event is triggered by an alarm. The action can be to generate a log entry, an SNMP trap, or both. You must define the events before an alarm can be configured. If you do not configure the RMON event first, you will receive an error when you configure the alarm settings.

By default, no RMON alarms and events are configured and RMON collection statistics are not enabled.

## Configuring RMON events

You can add or remove an event in the RMON event table that is associated with an RMON alarm number.

To configure RMON events, perform the following steps from privileged EXEC mode.

1. Enter the **configure terminal** command to access global configuration mode.

```
switch# configure terminal
```

2. Configure the RMON event.

```
switch(config)# rmon event 27 description Rising_Threshold log owner john_smith trap syslog
```

3. Return to privileged EXEC mode.

```
switch(config)# end
```

4. Save the *running-config* file to the *startup-config* file.

```
switch# copy running-config startup-config
```

## Configuring RMON Ethernet group statistics collection

You can collect RMON Ethernet group statistics on an interface. RMON alarms and events must be configured for you to display collection statistics. By default, RMON Ethernet group statistics are not enabled.

Ethernet group statistics collection is not supported on ISL links.

#### NOTE

RMON configuration is not supported on breakout ports in Network OS versions prior to v6.0.0.

To collect RMON Ethernet group statistics on an interface, perform the following steps from privileged EXEC mode.

1. Enter the **configure terminal** command to access global configuration mode.

```
switch# configure terminal
```

2. Enter the **interface** command to specify the interface type and RBridge-id/slot/port number.

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

3. Enable the DCB interface.

```
switch(config-if-te-1/0/1)# no shutdown
```

4. Configure RMON Ethernet group statistics on the interface.

```
switch(config-if-te-1/0/1)# rmon collection stats 200 owner john_smith
```

5. Return to privileged EXEC mode.

```
switch(config-if-te-1/0/1)# end
```

6. Enter the **copy** command to save the running-config file to the startup-config file.

```
switch# copy running-config startup-config
```

## Configuring RMON alarm settings

To configure RMON alarms and events, perform the following steps from privileged EXEC mode.

1. Enter the **configure terminal** command to access global configuration mode.

```
switch# configure terminal
```

2. Configure the RMON alarms.

Example of an alarm that tests every sample for a rising threshold

```
switch(config)# rmon alarm 5 1.3.6.1.2.1.16.1.1.1.5.65535 interval 30
                    absolute rising-threshold 95 event 27 owner john_smith
```

Example of an alarm that tests the delta between samples for a falling threshold

```
switch(config)# rmon alarm 5 1.3.6.1.2.1.16.1.1.1.5.65535 interval 10 delta
                    falling-threshold 65 event 42 owner john_smith
```

3. Return to privileged EXEC mode.

```
switch(config)# end
```

4. Save the *running-config* file to the *startup-config* file.

```
switch# copy running-config startup-config
```

5. To view configured alarms, use the **show running-config rmon alarm** command.

## Monitoring CRC errors

Certain interface counters, such as those for CRC errors, may not be available by means of SNMP OIDs. In this case it is recommended that either RMON or CLI be used to monitor those statistics.

The following synchronizes the statistics maintained for the interface and RMON, as well as ensures proper reporting from an operational standpoint.

1. First use the **clear counters all** command in global configuration mode.

```
device# clear counters all
```

2. Then use **the clear counters rmon** command.

```
device# clear counters rmon
```

3. Finally, execute the **rmon collection stats** command on each interface, as in the following example.

```
device(config)# interface tengigabitethernet 170/0/1  
device(conf-if-te-170/0/1)# rmon collection stats 2 owner admin
```

4. Use an appropriate RMON MIB for additional monitoring.

For example, to obtain CRC statistics on a Brocade VDX platform, the following RMON MIB could be used: Object-etherStatsCRCAAlignErrors, OID- .1.3.6.1.2.1.16.1.1.8



# Diagnostic Port

- Supported platforms for D\_Port..... 247
- Understanding D\_Port..... 247
- Topology 1: ISLs..... 250
- Using D\_Port in static-static mode between switches..... 250
- Using D\_Port in dynamic mode..... 253
- Managing D\_Port testing..... 255
- Using D\_Port show commands..... 255

## Supported platforms for D\_Port

D\_Port functionality is supported only on Brocade VDX platforms running Network OS 7.0.0 or later. Any port that can support ISL can support D\_Port. The following interfaces are also supported:

- 10-Gbps copper
- 10 Gbps
- 10 Gbps x 4 (breakout)
- 40 Gbps
- 100 Gbps

The following table lists the Brocade devices that support the D\_Port feature.

**TABLE 39** Supported platforms for D\_Port with Network OS

Product
Brocade VDX 2741
Brocade VDX 2746
Brocade VDX 6740
Brocade VDX 6740-T
Brocade VDX 6940-36Q
Brocade VDX 6940-72Q
Brocade VDX 6940-144S
Brocade VDX 8770-4
Brocade VDX 8770-8

**NOTE**

1-Gbps interfaces are not supported.

## Understanding D\_Port

A port in D\_Port mode does not carry any user traffic, and is designed to run only specific diagnostics tests for identifying link-level faults or failures.

To bring up a port in D\_Port mode, follow these basic steps:

1. Disable the ISL capability on the ports by issuing the **no fabric isl enable** command.
2. Enable D\_Port functionality on both ends of the link.

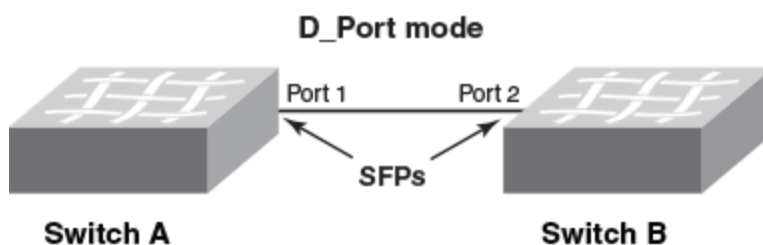
3. Enable the ISL capability on the ports by issuing the **fabric isl enable** command.

The following figure illustrates an example D\_Port connection between a pair of switches through SFP transceivers (port assignments will vary).

#### NOTE

For Network OS, D\_Ports are supported only on TRILL-capable links between two Network OS switches.

**FIGURE 42** Example of a basic D\_Port connection between switches



Once the ports are configured and enabled as D\_Ports, the following basic test suite is executed in the following order, depending on the SFPs installed:

1. Link traffic (for 10-Gbps SFPs, 10\*4-Gbps QSFPs, 40-Gbps SFPs, 100-Gbps SFPs)

The following steps are the fundamental parts of D\_Port testing:

1. The user configures the desired ports on either end, or both ends, of the connection. (The default D\_Port mode of a port is dynamic mode. If the user configures one end as D\_Port static mode, then the other end behaves as a D\_Port. Alternatively, the user can configure both ends as D\_Port static mode.)
2. Once both sides are configured, a basic test suite is initiated automatically when the link comes online, conducting diagnostic tests in the following order:
  - a. link traffic
3. After the automatic test is complete, the user can view results through the CLI or a GUI and rectify issues (if any) that are reported.
4. The user can also start (and restart) the test manually to verify the link.

## D\_Port configuration modes and testing

A D\_Port can be configured in the following modes:

- **Static** — The user explicitly configures the port as a D\_Port. In this mode, the port remains a D\_Port until you explicitly remove the D\_Port configuration. You must remove the D\_Port configuration at both ends of the link to bring up the port as a regular E\_Port.
- **Dynamic** — Dynamic testing is enabled by default. The port is automatically set to a D\_Port based on an external request from a remote port on the other end of the connection. The remote port must be a static D\_Port for testing to be performed. In dynamic mode, the port remains a D\_Port until all the diagnostic tests are completed and the remote port reverts to normal mode, coming up as a regular E\_Port or F\_Port. For the port to become a dynamic D\_Port, the remote port on the other end of the connection must be a static D\_Port.



- **None** — This mode prevents a test from running regardless of the configuration on the other end of the link.

When the tests complete, the port behavior depends on the mode:

- For static D\_Ports, you must remove the D\_Port configuration at either or both ends of the link to bring up the port as a regular E\_Port.
- For a switch port in dynamic D\_Port mode, the port automatically reverts back to an E\_Port if the port at the other end reverts to a regular port.

You can also manage aspects of the test. See "Managing D\_Port testing" later in this chapter.

## General limitations and considerations for D\_Port tests

Consider the following issues when running D\_Port tests:

- Testing is supported in management cluster and logical chassis cluster modes.
- D\_Port testing is not supported between Network OS Fibre Channel ports, including between an Access Gateway to Fabric OS connections and between ISLs and Fabric OS EX\_Port connections.
- The link to be tested must be marginally functional and able to carry a minimal number of frames before it can become a D\_Port link.
- D\_Port testing is useful for diagnosing marginal faults only. A complete failure of any component cannot be detected.
- Switches must be configured with the same VCS ID and the same default FCoE VLAN.
- Tests can be run within a cluster, as well as in a noncluster configuration. The switches are not required to be in the same cluster. Testing does not disrupt the cluster or fabric.
  - Within a cluster, disable the ISL (it must not be the only one if you want the cluster to stay up. Then set one or both sides to static mode and reenable the ISL. The test runs automatically.
  - In a noncluster configuration, no special configuration is required. Set the external switch to static mode to run tests on new ports in a cluster without disruption.
- You can configure multiple ports in parallel, in which case the tests are serialized. Keep in mind that the number of parallel ports and frame tests will affect the test time accordingly.
- Edge ports are not supported.
- Optical and electrical loopback tests are not supported for TRILL ISLs. Instead, Brocade spinFab creates a loopback route on both ends of the link, millions of frames are looped, and statistics are gathered.
- TRILL ISL ASIC limitations apply to supported tests.
- Before downgrading to a release that does not support D\_Port, the port type must be cleared of the D\_Port configuration.
- D\_Port configuration is not supported on mezzanine cards.
- D\_Ports do not support a loop topology.
- D\_Port testing is not supported on adapter ports configured in CNA mode.
- Toggling the port on either side of the link restarts the test.
- When a large number of D\_Ports are configured, the test is run on one port per blade at a time, and other ports wait until the test is completed. No test begins until the fabric is stable.

## High Availability limitations and considerations for D\_Ports

Consider the following High Availability (HA) limitations and considerations when using D\_Ports:

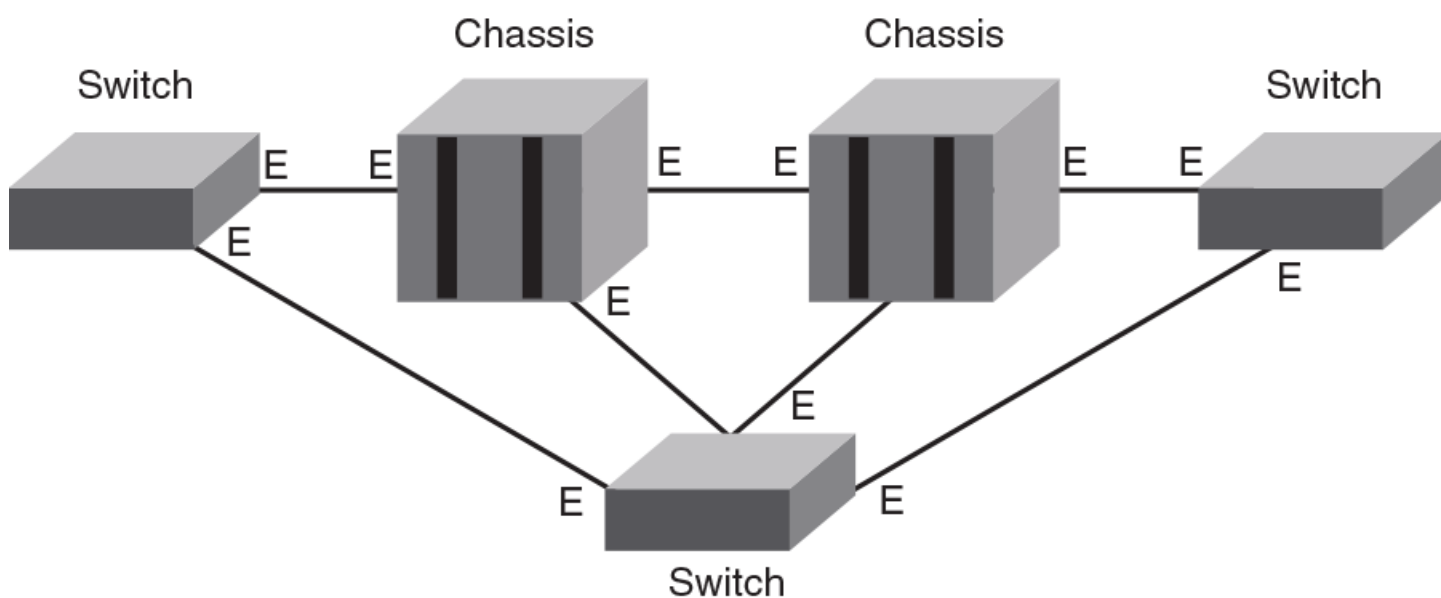
- There is no HA support for D\_Port test options and results. Any information from a previous test is lost following a failover or reboot.

- During an HA failover reboot on one side of the link, the link is reinitialized and may restart the test. However, the test cannot proceed if the remote port is not ready to proceed further (the remote port may already be done with the D\_Port test and in the final state). In such a case, the test will eventually fail with a "Remote port not ready" message. Restarting the test from either side will recover the port.

## Topology 1: ISLs

The following figure illustrates inter-switch links (ISLs) that connect multiple switches through a pair of chassis. The letter E represents E\_Ports to be configured as D\_Ports.

FIGURE 43 ISLs connecting multiple switches and chassis



Note the following:

- Only static-static and static-dynamic D\_Port modes are supported on the ISLs.

## Using D\_Port in static-static mode between switches

This section illustrates the configuration of static-static mode on ISLs for the illustrated topology.

### Enabling D\_Port in static mode

Use this procedure to configure a basic, automatic D\_Port diagnostics session in static mode between two switches. The summary steps are as follows:

1. Disable ISL functionality on the ports by running the **no fabric isl enable** command.
2. Configure D\_Port static mode on both ends of the link.

3. Enable ISL functionality on the ports by running the **fabric isl enable** command.

#### ATTENTION

The automatic test might fail if you do not follow the sequence of steps exactly.

#### NOTE

"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested.

1. Disable Port 1 on Switch A.

#### NOTE

This example uses TenGigabitEthernet ports.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)#
```

2. Configure Port 1 on Switch A as a D\_Port in static mode.

```
device(conf-if-te-52/0/35)# fabric dport mode static
device(conf-if-te-52/0/35)#
```

3. Repeat Step 1 and Step 2 for the corresponding port (in this example, Port 2) on Switch B.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)# fabric dport mode static
```

4. Reenable Port 1 on Switch A.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

5. Reenable Port 2 on Switch B.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

The basic test suite starts as soon as both ports are enabled and ready to perform the test.

#### NOTE

For the details of using the available nondefault test options, see the **diag dport-test** command.

6. To confirm D\_Port configuration on a port, as reflected in the running configuration, use the following command:

```
device(config)# sh run int te 1/2/8
interface TenGigabitEthernet 1/2/8
fabric isl enable
fabric trunk enable
fabric dport mode static
no shutdown
```

7. While the test is running, you can enter a variety of **show** commands to confirm the D\_Port configuration and view test results on an interface. See "Using D\_Port show commands" at the end of this chapter.

To view D\_Port status and test results for an interface:

```
device# show dport-test interface Tengigabitethernet 238/0/96
D-Port Information:
=====
Interface Name:                Te 238/0/96
Index:                          239
Remote Interface Name:         Te 24/0/2
Remote Index:                   145
Remote WWNN:                   10:00:00:05:33:e7:f0:d0
Mode:                           Automatic
No. of test frames:            1 Million
Test frame size:                1024 Bytes
Start time:                     Tue Feb  2 14:01:45 2016
End time:                       Tue Feb  2 14:02:27 2016
Status:                         PASSED
=====
Test                           Start time      Result          EST (HH:MM:SS)  Comments
=====
Link traffic test              14:02:18       PASSED         -----         -----
=====
```

## Disabling D\_Port in static mode

Use this procedure to disable a D\_Port diagnostics session in static mode, as configured in "Enabling D\_Port in static mode."

### NOTE

"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested.

1. Disable Port 1 on Switch A.

### NOTE

This example uses TenGigabitEthernet ports.

```
device# config
device(config)# int te 52/0/35
device(config-if-te-52/0/35)# no fabric isl enable
device(config-if-te-52/0/35)#
```

2. Disable the D\_Port functionality in static mode on Port 1 on Switch A.

```
device(config-if-te-52/0/35)# fabric dport mode none
device(config-if-te-52/0/35)#
```

3. Repeat Steps 1 and Step 2 for Port 2 on Switch B.

```
device# config
device(config)# int te 52/0/35
device(config-if-te-52/0/35)# no fabric isl enable
device(config-if-te-52/0/35)# fabric dport mode none
```

4. Reenable Port 1 on Switch A.

```
device(config-if-te-52/0/35)# fabric isl enable
device(config-if-te-52/0/35)#
```

## 5. Reenable Port 2 on Switch B.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

## Disabling D\_Port globally

You can prevent D\_Port testing from running regardless of the configuration at the other end of the link.

## 1. Enter interface subtype configuration mode.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)#
```

2. Enter the **fabric dport mode none** command.

```
device(conf-if-te-52/0/35)# fabric dport mode none
device(conf-if-te-52/0/35)#
```

## Using D\_Port in dynamic mode

Enabling dynamic D\_Port switch-wide configuration forces the ports on that switch or chassis to respond to D\_Port requests from the other end of the connection. It basically responds to a remote port request to change its mode to D\_Port mode, and run diagnostic tests automatically. For more information on enabling dynamic D\_Port mode for all ports in a switch or chassis, refer to "D\_Port configuration mode and testing" in this chapter.

## Enabling D\_Port in dynamic mode

Use this procedure to configure a basic D\_Port diagnostics session in dynamic mode between two switches. The summary steps are as follows:

1. Disable the ports on both ends of the link.
2. Configure D\_Port dynamic mode on both ends of the link.
3. Enable the ports on both ends of the link.

### ATTENTION

The automatic test might fail if you do not follow the sequence of steps exactly. You must also disable dynamic mode on a port if you want that port never to become a D\_Port.

### NOTE

"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested.

1. Disable Port 1 on Switch A.

### NOTE

This example uses TenGigabitEthernet ports.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
```

```
device(conf-if-te-52/0/35)#
```

2. Configure Port 1 on Switch A as a D\_Port in dynamic mode.

```
device(conf-if-te-52/0/35)# fabric dport mode dynamic
device(conf-if-te-52/0/35)#
```

3. Repeat Step 1 and Step 2 for the corresponding port (in this example, Port 2) on Switch B.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)# fabric dport mode dynamic
```

4. Reenable Port 1 on Switch A.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

5. Reenable Port 2 on Switch B.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

The basic test suite starts as soon as both ports are enabled and ready to perform the test.

6. While the test is running, enter the following **show** command to view test results. The following test is successful.
7. To display a summary of the D\_Port, use the following command.

## Disabling D\_Port in dynamic mode

Use this procedure to disable a D\_Port diagnostics session in dynamic mode, as configured in "Enabling D\_Port in dynamic mode."

### NOTE

"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested.

### ATTENTION

You must also disable dynamic mode on a port if you want that port never to become a D\_Port.

1. Disable Port 1 on Switch A.

### NOTE

This example uses TenGigabitEthernet ports.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)#
```

2. Disable the D\_Port functionality in dynamic mode on Port 1 on Switch A.

```
device(conf-if-te-52/0/35)# fabric dport mode none
device(conf-if-te-52/0/35)#
```

- Repeat Steps 1 and Step 2 for Port 2 on Switch B.

```
device# config
device(config)# int te 52/0/35
device(conf-if-te-52/0/35)# no fabric isl enable
device(conf-if-te-52/0/35)# fabric dport mode none
```

- Reenable Port 1 on Switch A.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

- Reenable Port 2 on Switch B.

```
device(conf-if-te-52/0/35)# fabric isl enable
device(conf-if-te-52/0/35)#
```

## Managing D\_Port testing

You can start, stop, and restart diagnostic testing on a port enabled as a D\_Port (diagnostic port), as well as specify the frame size and number of frames to be transmitted in testing

The **diag dport-test interface** command provides the above options, as illustrated in the following example. For command details, see the *Network OS Command Reference*.

The following starts D\_Port testing on a TenGigabitEthernet port and sets the number of frames to 2,000,000 and the frame size to 1800 bytes.

```
device# diag dport-test interface TenGigabitEthernet 51/0/13 start nframe 2 framesize 1800

=====
Interface          Status
=====
Te 51/0/13         Test started. To view results run "show dport-test interface Te 51/0/13"
=====
```

### NOTE

As noted in the test response, you can use the **show dport-test interface** command to view the results.

## Using D\_Port show commands

This section presents a variety of options for viewing the results of D\_Port testing.

The global **show running config interface** command shows the status of the D\_Port test configuration on the configured port.

```
device# show running-config interface TenGigabitEthernet 52/0/35
interface TenGigabitEthernet 52/0/35
fabric isl enable
fabric trunk enable
fabric dport mode none
no shutdown
```

Use the above command in interface subtype configuration mode to see the same results.

```
device(conf-if-te-52/0/35)# do show running-config interface TenGigabitEthernet 52/0/35
interface TenGigabitEthernet 52/0/35
fabric isl enable
fabric trunk enable
```

```
fabric dport mode none
no shutdown
```

Use the **show dport-test interface** command to display basic test results for a specified interface.

```
show dport-test interface Tengigabitethernet 56/0/1
D-Port Information:
=====
Interface Name:          Te 56/0/1
Index:                   64
Remote Interface Name:  Te 60/4/1
Remote Index:            12
Remote WWNN:             10:00:00:27:f8:1e:aa:48
Mode:                    Automatic
No. of test frames:     1 Million
Test frame size:        1024 Bytes
Start time:              Tue Feb  2 04:44:33 2016
End time:                Tue Feb  2 04:44:47 2016
Status:                  PASSED
=====
Test                      Start time      Result          EST(HH:MM:SS)  Comments
=====
Link traffic test         04:44:36       PASSED         -----        -----
=====
```

Use the **show dport-test interface detail** command to display test results for the interface, as well as frame statistics for the port under test and any detailed errors.

#### NOTE

Statistics are cleared before a new test is started. The log is empty for a successful test.

```
device# show dport-test interface Tengigabitethernet 56/0/1 detail
D-Port Information:
=====
Interface Name:          Te 56/0/1
Index:                   64
Remote Interface Name:  Te 60/4/1
Remote Index:            12
Remote WWNN:             10:00:00:27:f8:1e:aa:48
Mode:                    Automatic
No. of test frames:     1 Million
Test frame size:        1024 Bytes
Start time:              Tue Feb  2 04:44:33 2016
End time:                Tue Feb  2 04:44:47 2016
Status:                  PASSED
=====+
Test                      Start time      Result          EST(HH:MM:SS)  Comments
=====
Link traffic test         04:44:36       PASSED         -----        -----
=====
D-Port statistics:
=====
                RX                                TX
Packets         3299499                            3300600
Bytes           3602996140                          3603243530
Unicasts        3299442                              3300533
Multicasts      57                                     67
Broadcasts      0                                       0
Errors           0                                       0
Discards        0                                       0
Overruns        0          Underruns                    0
Runts           0
Jabbers         0
CRC             0
64-byte pkts   0
Over 64-byte pkts 46
Over 127-byte pkts 10
Over 255-byte pkts 1
Over 511-byte pkts 1
Over 1023-byte pkts 3299441
```



```

Over 1518-byte pkts          0
Mbits/Sec                   0.000000          0.000000
Packet/Sec                   0
Line-rate                   0.00%           0.00%

```

```

=====
Spinfab Log:
=====

```

```

Logs Unavailable

```

Use the **show dport-test rbridge-id** command to display summary test results for all D\_Ports in a specified RBridge.

```

device# show dporttest rbridge-id 56

```

```

RBridge-Id : 56

```

```

=====
Index  Interface      State      D-Port Mode      Test Result
=====
64     Te 56/0/1        ONLINE    Static            PASSED
87     Te 56/0/24       ONLINE    Static            PASSED
=====

```

#### NOTE

The **rbridge-id all** option is not supported.

Use the **show dport-test all** command to display test results for all D\_Ports in the fabric.

```

device# show dport-test all

```

```

RBridge-Id : 60

```

```

=====
Index  Interface      State      D-Port Mode      Test Result
=====
12     Te 60/4/1       ONLINE    Dynamic           PASSED
=====

```

```

RBridge-Id : 55

```

```

=====
Index  Interface      State      D-Port Mode      Test Result
=====
86     Te 55/0/23     ONLINE    Dynamic           PASSED
=====

```

```

RBridge-Id : 56

```

```

=====
Index  Interface      State      D-Port Mode      Test Result
=====
64     Te 56/0/1        ONLINE    Static            PASSED
87     Te 56/0/24       ONLINE    Static            PASSED
=====

```



# Python Event-Management and Scripting

• Python under Network OS .....	259
• Implementing Python scripts .....	260
• Implementing Python event-management .....	269
• Troubleshooting event-management.....	272
• Event-management show commands .....	272

## Python under Network OS

The Python interpreter installed with Network OS enables you to access a Python shell or to launch Python scripts. You can also define event handlers that run such scripts automatically upon specified conditions.

### Python overview

Python is a high-level scripting language that also supports object-oriented programming. If you have previous programming experience, you can quickly learn how to write useful, simple Python scripts.

#### NOTE

For Python resources, refer to <http://python.org>.

### Working interactively in the Python shell

Use this procedure to access a Python shell, within which you can use Python commands that call and manipulate Network OS commands.

#### NOTE

The Python shell is accessible only to admin-role users.  
Python syntax is case-sensitive.

1. In privileged EXEC mode, enter **python** to access the Python shell.

```
device# python
```

The device# prompt changes to a Python prompt:

```
Python 3.3.2 (default, Jun 5 2013, 11:04:06)
[GCC 4.3.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

2. To exit the Python shell and return to the Network OS prompt, enter either:
  - `exit()`
  - `Ctrl-D`
3. To run a Network OS command from within the Python shell, enter the `CLI()` command.

```
>>> cmd_show_running_vlan = CLI('show running-config interface vlan')
!Command: show running-config interface vlan
!Time: Tue Jan 6 00:12:37 2015
interface Vlan 1
>>>
```

The statement entered above does two things:

- Runs the **show running-config interface vlan** command and displays the result.
- Assigns that command to a Python variable named `cmd_show_running_vlan`

4. To run a series of Network OS commands from within the Python shell, separate the commands with `\n`.

```
>>> cmd_config_vlans = CLI('configure \n interface vlan 101-103 \n exit')
!Command: configure \n interface vlan 101-103 \n exit
!Time: Tue Jan 6 00:24:17 2015
>>>
```

#### NOTE

There is a difference between running a sequence of Network OS CLI commands in the Python shell rather than in the standard Network OS interface. Whereas in the standard interface the result of a command is persistent, in the Python shell each `CLI( )` statement is independent of any preceding ones.

In the following example, the lines beginning with **#** are added for explanation.

```
device# python
Python 3.3.2 (default, Jun 5 2013, 11:04:06)
[GCC 4.3.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_show_running_vlan = CLI('show running-config interface vlan')
# The Network OS show running-config int vlan command is run,
# and that command is assigned to the Python variable cmd_show_running_vlan.
!Command: show running-config interface vlan
!Time: Tue Jan 6 00:12:37 2015
interface Vlan 1
!
>>> cmd_config_vlans = CLI('configure \n interface vlan 101-103 \n exit')
# A series of three commands are run and assigned to the Python variable cmd_config_vlans.
!Command: configure \n interface vlan 101-103 \n exit
!Time: Tue Jan 6 00:24:17 2015

>>> cmd_show_running_vlan.rerun()
# The rerun() function appended to cmd_show_running_vlan gives the following output:
!Command: show running-config interface vlan
!Time: Tue Jan 6 00:24:34 2015
interface Vlan 1
!
interface Vlan 101
!
interface Vlan 102
!
interface Vlan 103
!
```

## Implementing Python scripts

Python scripts enable you to manipulate and launch Network OS commands, taking advantage of the power and flexibility of Python. Such scripts also support event handling.

The topics in this section guide you through the process of writing and testing Python scripts, copying them to supported devices, and running them from the command line.

#### NOTE

This section is also required for [Implementing Python event-management](#) on page 269.

## Guidelines for writing Python scripts

The guidelines for writing Python scripts to run under Network OS are as follows:

- Although previous experience programming in Python is helpful, experience in other high-level languages is enough to get you started with simple Python scripts.
- The Python developer either needs experience with Network OS CLI or access to a resource with such experience.
- To help decide which editor or integrated development environment (IDE) to use, refer to <http://www.python.org>.
- Make sure that the appropriate version of the Python interpreter is installed on your development computer. For Network OS 7.0.0, install Python 3.3.2.
- Make sure that in the *Network OS Command Reference* you are familiar with the **python** and the **CLI()** topics.
- One of the first statements in the script should be `from CLI import CLI`. This enables the `CLI()` command, by which Python can interact with Network OS.
- Write the Python script and save it, with a `.py` suffix. Valid filenames range from 4 through 32 characters (including the suffix). The first character must be alphabetic.

### NOTE

For additional sample scripts, refer to [Python scripts and run-logs](#) on page 263.

## Testing Python-script statements

While developing a Python script, you can test Network OS calls by entering them in the switch Python command shell. After the script is stable, you copy it to the switch and then test it further by running it from the command line.

1. In privileged EXEC mode, enter the **python** command to access the Python shell.

```
device# python

Python 3.3.2 (default, Jun 5 2013, 11:04:06)
[GCC 4.3.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Note that the `device#` prompt changed to a `>>>` Python prompt:

2. Enter the script statements one at a time, verifying that they run as expected.

```
>>> cmd_config_vlans = CLI('configure \n interface vlan 101-103 \n exit')
!Command: configure \n interface vlan 101-103 \n exit
!Time: Tue Jan 6 00:24:17 2015
>>>
```

3. Make corrections as needed.

## Copying Python files to switches

After writing and testing a Python script file, use one of these procedures to copy it to switch flash memory.

### Copying a file from a USB device to a switch

Use this procedure to copy a file from a USB device to a switch.

#### ATTENTION

The only supported USB device for this procedure is the Brocade USB device shipped with the switch.

1. Copy the Python script file to a USB storage device.
2. Insert the USB device into the switch USB port and enter the **usb on** command.
3. In privileged EXEC mode, enter the **copy** command to copy the Python file from the USB device to the switch flash memory.

```
device# copy usb://pythscript1.py flash://pythscript1.py
```

4. To display a list of files in the switch flash memory, enter the **dir** command.

```
device# dir
total 24
drwxr-xr-x  2 root    sys      4096 Mar 26 15:22 .
drwxr-xr-x  3 root    root     4096 Jan  1  1970 ..
-rw-r--r--  1 root    root     1051 Mar 24 16:09 create_po.py
-rw-r--r--  1 root    root     207  Mar 24 16:09 create_vlans.py
-rw-r--r--  1 root    sys      557  Mar 26 10:37 defaultconfig.novcs
-rw-r--r--  1 root    sys      778  Mar 26 10:37 defaultconfig.vcs

1922789376 bytes total (828317696 bytes free)
```

5. To display the contents of a Python file copied into the switch flash memory, enter the **show file** command.

```
device# show file pythscript1.py
```

## Downloading a file from a network to a switch

Use this procedure to download a file from a network location to a switch.

1. Make sure that the Python script file is uploaded to an accessible network location.
2. In privileged EXEC mode, enter the **copy** command to copy the Python file from the network location to the switch flash memory.

```
device# copy ftp://MyUserID:MyPassword@10.10.10.10//pythscript1.py flash://pythscript1.py
```

For other file-transfer options, refer to the *Network OS Command Reference* **copy** topic.

3. To display a list of files in the switch flash memory, enter the **dir** command.

```
device# dir
total 24
drwxr-xr-x  2 root    sys      4096 Mar 26 15:22 .
drwxr-xr-x  3 root    root     4096 Jan  1  1970 ..
-rw-r--r--  1 root    root     1051 Mar 24 16:09 create_po.py
-rw-r--r--  1 root    root     207  Mar 24 16:09 create_vlans.py
-rw-r--r--  1 root    sys      557  Mar 26 10:37 defaultconfig.novcs
-rw-r--r--  1 root    sys      778  Mar 26 10:37 defaultconfig.vcs

1922789376 bytes total (828317696 bytes free)
```

4. To display the contents of a Python file copied into the switch flash memory, enter the **show file** command.

```
device# show file pythscript1.py
```

## Running Python scripts from the command line

The facility to run Python scripts from the Network OS command line enables you to execute complex and repetitious tasks with accuracy and efficiency. This facility also enables you to validate scripts intended for event management.



### CAUTION

Make sure that you test Python scripts according to standard quality assurance practices before deploying them.

**NOTE**

To perform this procedure, you need admin-role access.

In privileged EXEC mode, enter the **python** command, specifying the Python script file that you want to run.

```
device# python create_po.py
```

**NOTE**

The `create_po.py` script is discussed in [Script for assigning interfaces to port channels \(create\\_po.py\)](#) on page 263.

## Python scripts and run-logs

This section contains sample Network OS Python scripts and run-logs.

### Script for assigning interfaces to port channels (create\_po.py)

The `create_po.py` script is an example for automating common configuration tasks.

#### Script (create\_po.py)

This script runs the relevant **show running-config** commands before and after the following actions:

- VLAN configuration
- Port-channel configuration
- Adding interfaces to port channels

**NOTE**

Lines beginning with # are annotations.

```
#Required in all scripts for NOS:
from CLI import CLI

rbridges = [3, 4]
interfaces = [40, 41, 42, 43]
port_channel = 10
vlan_range = "101-105"
slot_number = 0

# Runs show running-config int vlan before the configuration, and assigns this NOS
# command to a Python variable named cmd_show_running_vlans.
cmd_show_running_vlans = CLI("show running-config int vlan")

# Configures VLANs. {} is a placeholder for the format (arg1, arg2, ... argN) variables:
cmd_configure_vlans = CLI("config \n int vlan {}".format(vlan_range))

# Reruns show running-config int vlan, following definition of new VLANs:
cmd_show_running_vlans.rerun()

# Configures port channel (vLAG):
cmd_show_running_port_channels = CLI("show running-config int po")
cmd_configure_port_channel = CLI("config \n int po {} \n switchport \n switchport mode trunk \n switchport trunk allowed vlan add {} \n switchport trunk tag native-vlan ; no shut".format(port_channel, vlan_range))

# Reruns show running-config int po, following configuration changes:
cmd_show_running_port_channels.rerun()

# Add interfaces to port channel (vLAG)
for rbridge in rbridges:
    for interface in interfaces:
        cmd_configure_interface = CLI("config \n int te {}/{} /{} \n fabric isl enable \n fabric trunk enable \n channel-group {} mode active type standard \n no shut".format(rbridge, slot_number, interface, port_channel))
```

```

cmd_show_running_int_tengig = CLI("show running-config int te {}/{}/{}/{}".format (rbridge,
slot_number, interface))

# Runs show running-config:
cmd_show_running = CLI("show running-config")

```

### Run-log (create\_po.py)

A log upon running create\_po.py was as follows:

```

device# python create_po.py
!Command: show running-config int vlan
!Time: Mon May 18 15:08:52 2015

interface Vlan 1
!
!Command: config
int vlan 101-105
!Time: Mon May 18 15:08:52 2015

!Command: show running-config int vlan
!Time: Mon May 18 15:08:53 2015
interface Vlan 1
!
interface Vlan 101
!
interface Vlan 102
!
interface Vlan 103
!
interface Vlan 104
!
interface Vlan 105
!

!Command: show running-config int po
!Time: Mon May 18 15:08:54 2015

% No entries found.

!Command: config
int po 10
switchport
switchport mode trunk
switchport trunk allowed vlan add 101-105
switchport trunk tag native-vlan ; no shut
!Time: Mon May 18 15:08:54 2015

!Command: show running-config int po
!Time: Mon May 18 15:08:56 2015

interface Port-channel 10
vlag ignore-split
switchport
switchport mode trunk
switchport trunk allowed vlan add 101-105
switchport trunk tag native-vlan
spanning-tree shutdown
no shutdown
!
!Command: config
int te 3/0/40
fabric isl enable
fabric trunk enable
channel-group 10 mode active type standard
no shut
!Time: Mon May 18 15:08:57 2015

!Command: show running-config int te 3/0/40
!Time: Mon May 18 15:08:59 2015

```



```

interface TenGigabitEthernet 3/0/40
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  lacp timeout long
  no shutdown
!
!Command: config
  int te 3/0/41
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  no shut
!Time: Mon May 18 15:09:00 2015

!Command: show running-config int te 3/0/41
!Time: Mon May 18 15:09:01 2015

interface TenGigabitEthernet 3/0/41
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  lacp timeout long
  no shutdown
!
!Command: config
  int te 3/0/42
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  no shut
!Time: Mon May 18 15:09:03 2015

!Command: show running-config int te 3/0/42
!Time: Mon May 18 15:09:05 2015

interface TenGigabitEthernet 3/0/42
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  lacp timeout long
  no shutdown
!
!Command: config
  int te 3/0/43
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  no shut
!Time: Mon May 18 15:09:06 2015

!Command: show running-config int te 3/0/43
!Time: Mon May 18 15:09:07 2015

interface TenGigabitEthernet 3/0/43
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  lacp timeout long
  no shutdown
!
!Command: config
  int te 4/0/40
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  no shut
!Time: Mon May 18 15:09:08 2015

!Command: show running-config int te 4/0/40
!Time: Mon May 18 15:09:10 2015

```

```

interface TenGigabitEthernet 4/0/40
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  lACP timeout long
  no shutdown
!
!Command: config
  int te 4/0/41
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  no shut
!Time: Mon May 18 15:09:11 2015

!Command: show running-config int te 4/0/41
!Time: Mon May 18 15:09:12 2015

interface TenGigabitEthernet 4/0/41
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  lACP timeout long
  no shutdown
!
!Command: config
  int te 4/0/42
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  no shut
!Time: Mon May 18 15:09:13 2015

!Command: show running-config int te 4/0/42
!Time: Mon May 18 15:09:15 2015

interface TenGigabitEthernet 4/0/42
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  lACP timeout long
  no shutdown
!
!Command: config
  int te 4/0/43
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  no shut
!Time: Mon May 18 15:09:16 2015

!Command: show running-config int te 4/0/43
!Time: Mon May 18 15:09:17 2015

interface TenGigabitEthernet 4/0/43
  fabric isl enable
  fabric trunk enable
  channel-group 10 mode active type standard
  lACP timeout long
  no shutdown
!
!Command: show running-config
!Time: Mon May 18 15:09:18 2015

diag post rbridge-id 1 enable
diag post rbridge-id 2 enable
diag post rbridge-id 3 enable
diag post rbridge-id 4 enable
hardware
  connector-group 2/0/1
    speed LowMixed

```



```
print('vcs_status: ', vcs_status)
print('fabric_status: ', fabric_status)
print('hostnames: ', hostnames)
```

## Run-log (get\_output.py)

A log upon running `get_output.py` was as follows:

```
device# python get_output.py
rbridges: ['2']
wwns: ['10:00:00:05:33:65:ED:F0']
mgmt_ip_addresses: ['10.24.81.101']
vcs_status: ['Online']
fabric_status: ['Online']
hostnames: ['sw0']
```

## Script for upgrading and reconfiguring switches (dad.py)

The `dad.py` script configures an RBridge or all VCS RBridges using DHCP automatic deployment (DAD).

### Script (dad.py)

This example configures an RBridge or all of the RBridges in a VCS using DHCP automatic deployment (DAD). The `python dad.py` command calls this script. Lines beginning with `#` are annotations.

#### ATTENTION

This script is run automatically by the DAD process. Refer to the "Using DHCP Automatic Deployment" section of the *Network OS Administration Guide*.

```
##
# Usage:
# dad.py -h | --help      help message
#          -g | --global  option for LC mode to set cluster global config
#          -r | --rbridgeid <#> option for LC mode and FC mode to set switch-specific config
#          -l | --local  otp option for LC mode to set switch-specific config
#
import os
import sys, getopt

# Import Network OS Python CLI module
from CLI import CLI

# debug log
log=open("/tmp/dadscript.log", "a")

def main(argv):
    mode = -1 # 0 - global, 1 - local
    rbridgeid = 0
    localcmd = 0 # local command
    try:
        opts, args = getopt.getopt(argv,"ghr:l",["global", "help", "rbridgeid=", "local"])
    except getopt.GetoptError:
        log.write('dad2.py [-h|--help] [-g|--global] [-r|--rbridgeid <#>] [-l|--local]\n')
        sys.exit(2)

# Parsing options
for opt, arg in opts:
    if opt in ("-g", "--global"):
        if len(opts) > 1:
            log.write("only one option is allowed\n")
            sys.exit(3)
        mode = 0
    elif opt in ("-r", "--rbridgeid"):
        mode = 1
        rbridgeid = int(arg)
    elif opt in ("-l", "--local"):
```

```

        if len(opts) == 1:
            log.write("-r is required\n")
            sys.exit(4)
        mode = 1
        localcmd = 1
    else:
        log.write('dad2.py [-h|--help] [-g|--global] [-r|--rbridgeid] [-l|--local]\n')
        sys.exit(1)
log.write("mode = " + str(mode) + '\n')

# Execute command
if mode == 0:
    log.write("apply global config\n")
    CLI("conf ; banner login DAD ; end")
elif localcmd == 0:
    log.write("apply local config\n")
    log.write("rbridgeid = " + str(rbridgeid) + '\n')
    CLI("conf ; rbridge-id " + str(rbridgeid) " ; switch-attributes host-name sw " + str(rbridgeid) +
" ; end")
else: # localcmd == 1
    log.write("apply local command\n")
    log.write("rbridgeid = " + str(rbridgeid) + '\n')
    os.system("date > /tmp/localcmd.date")
if __name__ == "__main__":
    main(sys.argv[1:])

```

### Run-log (dad.py)

The following are logs of running `dad.py` with various parameters.

#### NOTE

Because `dad.py` is run automatically by the DAD process, you need to enter **show dadstatus** in order to see the results.

The following command runs the `dad.py` script and sets the switch login banner to "DAD".

```

device# python dad.py -g
!Command: conf ; banner incoming DAD0 ; end
!Time: Thu Apr 16 00:06:35 2015

device#

```

The following command runs the `dad.py` script on RBridge 90, and sets the switch hostname to `sw90.0`:

```

device# python dad.py -r 90
!Command: conf ; rbridge-id 90 ; root en ; switch-attributes host-name sw90.0 ; end
!Time: Thu Apr 16 00:06:39 2015

device#

```

The following command runs the `dad.py` script on RBridge 90, and runs a Linux command to log the current time into `/tmp/localcmd.date`, with no monitor output:

```

device# python dad.py -r 90 -l

device#

```

## Implementing Python event-management

Python event management enables you to specify a Python script that runs automatically upon specified conditions.

The conditions available for triggering a Python script are as follows:

- A specified RASlog message
- One of the following switch events:

- Switch bootup
- Completion of cluster formation and completion of configuration-file replay

## Configuring an event-handler profile

Use this procedure to create an event-handler profile, define one or more triggers for it, and specify a Python script that runs upon one or more trigger events.

Before you begin, make sure you have performed [Implementing Python scripts](#) on page 260.

1. Enter **configure terminal** to access global configuration mode.

```
device# configure terminal
```

2. Enter the **event-handler** command.

```
device(config)# event-handler eventHandler1
```

3. For each trigger that you need for a profile, enter the **trigger** command.

```
device(config-event-handler-eventHandler1)# trigger 1 raslog LOG-1001
```

The trigger event is RASlog message #LOG-1001.

4. Enter the **action python-script** command to specify a Python script that runs when the event-handler is triggered.

```
device(config-event-handler-eventHandler1)# action python-script example.py
```

5. To add an event-handler-profile description, enter **description**, followed by the description text.

```
device(config-event-handler-eventHandler1)# description This is a sample description.
```



### CAUTION

Make sure that you test Python scripts according to standard quality assurance practices before deploying them.

The following example includes all of the above steps.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)# trigger 1 raslog LOG-1001
device(config-event-handler-eventHandler1)# action python-script example.py
device(config-event-handler-eventHandler1)# description This is a sample description.
```

## Activating an event-handler on an RBridge

Use this procedure to activate one or more event-handlers on an RBridge. If a trigger specified in the event-handler profile occurs, a designated Python script runs.

1. Enter **configure terminal** to access global configuration mode.

```
device# configure terminal
```

2. Enter the **rbridge-id** command to access RBridge configuration mode.

```
device(config)# rbridge-id 1
```

3. Enter the **event-handler activate** command, specifying the event handler that you are activating on the RBridge.

```
device(config-rbridge-id-1)# event-handler activate eventHandler1
```

- To activate an additional event handler on the RBridge, enter the **event-handler activate** command, specifying the additional event handler.

```
device(config-activate-eventHandler1)# event-handler activate eventHandler2
```

- To de-activate an event handler on that Rbridge, enter the **no event-handler activate** command

```
device(config-activate-eventHandler2)# no event-handler activate eventHandler2
```

The following example includes all of the activation steps.

```
device# configure terminal
device(config)# rbridge-id 1
device(config-rbridge-id-1)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# event-handler activate eventHandler2
```

## Configuring event-handler options

After you activate an event handler on a RBridge, you can configure various options. For example, you can specify if the event-handler script runs more than once and how multiple triggers are handled.

- Activate an event handler on an RBridge, as described in [Configuring an event-handler profile](#) on page 270:

```
device# configure terminal
device(config)# rbridge-id 1
device(config-rbridge-id-1)# event-handler activate eventHandler1
```

- To specify a delay from when a trigger is received until execution of the event-handler action, enter the **delay** command.

```
device(config-activate-eventHandler1)# delay 60
```

The above example specifies a delay of 60 seconds.

- To specify multiple iterations of the action when a trigger is received:

- Enter the **iterations** command.
- To specify an interval between iterations, enter the **interval** command.

```
device(config-event-handler-eventHandler1)# iterations 3
device(config-activate-eventHandler1)# interval 30
```

The above example sets the number of iterations to 3 and specifies an interval of 30 seconds between each iteration.

- To specify that a triggered action not be interrupted by cluster formation, enter the **run-mode exclusive** command.

```
device(config-activate-eventHandler1)# run-mode exclusive
```

- To specify a maximum number of minutes to wait for an action script to complete execution, enter the **action-timeout** command.

```
device(config-activate-eventHandler1)# action-timeout 30
```

The above example sets the timeout to 30 minutes.

- To limit action-recurrence upon multiple trigger-events, enter one of the following commands:

- trigger-mode only-once**—for the duration of a switch's configuration, the event-handler action is launched only once.

```
device(config-activate-eventHandler1)# trigger-mode only-once
```

- **trigger-mode on-first-instance**—as long as the switch is running, the event-handler action is launched only once. Following a switch restart, the event-handler action can be triggered again.

```
device(config-activate-eventHandler1)# trigger-mode on-first-instance
```

7. If multiple triggers are defined, to specify that the action run only if all of the triggers occur, enter the **trigger-function AND time-window** command.

```
device(config-activate-eventHandler1)# trigger-function AND time-window 120
```

The above example specifies that the action run only if all triggers occur within 120 seconds.

## Troubleshooting event-management

Use these topics to troubleshoot issues that arise during implementation of Python event-management.

### Aborting an event-handler action

If needed, abort a Python script launched by an event-handler action.

1. In privileged EXEC mode, enter the **event-handler abort action** command.

```
device# event-handler abort action eh1
This operation will abort an event handler action that is currently running and may leave the switch
in an inconsistent state. Do you want to continue? [y/n]:y
```

2. To confirm aborting the action, type *y*.

```
Operation completed successfully.
```

The Python script launched by the event-handler action is aborted.

## Event-management show commands

There are several **show** commands that display event-management information. They are documented in the *Network OS Command Reference*, and listed here with descriptions.

**TABLE 40** Event-management show commands in the *Network OS Command Reference*

Command	Description
<b>show event-handler activations</b>	Displays operational data of activated event-handlers.
<b>show running-config event-handler</b>	Displays details of event-handler profiles defined on the switch. You can display the results by description, Python-script action, or trigger ID.
<b>show running-config rbridge-id event-handler</b>	Displays one or all of the event-handlers in the running configuration. You can limit the display by RBridge ID, event-handler activation, and additional parameters.