

53-1002165-05
21 December 2011



Fabric OS

Documentation Updates

Supporting Fabric OS v7.0.x

BROCADE

Copyright © 2011 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCFM, DCX, Fabric OS, FastIron, IronView, NetIron, SAN Health, ServerIron, TurboIron, and Wingspan are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, Extraordinary Networks, MyBrocade, and VCS are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

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. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book 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>.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 - 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
<i>Fabric OS Documentation Updates</i>	53-1002165-01	New document	June 2011
<i>Fabric OS Documentation Updates</i>	53-1002165-02	Update to include FCIP Administrator's Guide correction	July 2011
<i>Fabric OS Documentation Updates</i>	53-1002165-03	Updates to CEE Command Reference, Encryption (RKM), Fabric Watch, FOS Administrators, and Troubleshooting guides.	August 2011
<i>Fabric OS Documentation Updates</i>	53-1002165-04	Updates to 6510, 8510-8, 8510-4, DCX, and DCX-4S hardware manuals.	September 2011
<i>Fabric OS Documentation Updates</i>	53-1002165-05	Updates to support Fabric OS 7.0.1.	December 2011

Contents

About This Document

In this chapter vii
How this document is organized vii
What’s new in this document..... viii
Brocade Resources ix
Document feedback ix

Chapter 1 Access Gateway Administrator’s Guide

In this chapter 1
Documentation updates for Fabric OS v7.0.0 and later 1
 Chapter 2, Configuring Ports in Access Gateway Mode 1

Chapter 2 CEE Command Reference

In this chapter 3
Documentation updates for Fabric OS v7.0.0 and later 3

Chapter 3 Fabric OS Administrator’s Guide

In this chapter 5
Documentation updates for Fabric OS v7.0.0 and later 5
 Chapter 22, Managing Long Distance Fabrics..... 5
Documentation updates for Fabric OS v7.0.1 and later 6
 Chapter 23, Managing Long Distance Fabrics..... 6

Chapter 4 Fabric OS Command Reference

In this chapter 7
Documentation Updates for Fabric OS v7.0.1..... 7
Documentation Updates for Fabric OS v7.0.0..... 9

Chapter 5 Fabric OS Encryption Guide Supporting LKM

In this chapter 13

	Documentation updates for LKM.	13
	Chapter 3, Configuring Brocade Encryption Using CLI	13
	Failover/failback policy configuration.	13
	Chapter 5, Best Practices and Special Topics	13
	Key Vault Best Practices	13
	Chapter 6, Maintenance and Troubleshooting.	13
	Manually synchronizing the security database	13
Chapter 6	Fabric OS Encryption Guide Supporting RKM	
	In this chapter	15
	Documentation updates for RKM	15
	Chapter 2, Encryption configuration using the Management application	15
	Disk device decommissioning.	15
	Chapter 3, Configuring Brocade Encryption Using CLI	16
	Failover/failback policy configuration.	16
	Chapter 5, Best Practices and Special Topics	17
	Key Vault Best Practices	17
	Chapter 6, Maintenance and Troubleshooting.	17
	Manually synchronizing the security database	17
Chapter 7	Fabric OS Encryption Guide Supporting SKM and ESKM	
	In this chapter	19
	Documentation updates for SKM	19
	Chapter 3, Configuring Brocade Encryption Using CLI	19
	Failover/failback policy configuration.	19
	Chapter 5, Best Practices and Special Topics	19
	Key Vault Best Practices	19
	Chapter 6, Maintenance and Troubleshooting.	19
	Manually synchronizing the security database	19
Chapter 8	Fabric OS Encryption Guide Supporting TEMS	
	In this chapter	21
	Documentation updates for TEMS.	21
	Chapter 3, Configuring Brocade Encryption Using CLI	21
	Failover/failback policy configuration.	21
	Chapter 5, Best Practices and Special Topics	21
	Key Vault Best Practices	21
	Chapter 6, Maintenance and Troubleshooting.	21
	Manually synchronizing the security database	21
Chapter 9	Fabric OS Encryption Guide Supporting TEMS	
	In this chapter	23

	Documentation updates for TKLM.	23
	Chapter 3, Configuring Brocade Encryption Using CLI	23
	Failover/failback policy configuration.	23
	Chapter 5, Best Practices and Special Topics	23
	Key Vault Best Practices	23
	Chapter 6, Maintenance and Troubleshooting.	23
	Manually synchronizing the security database	23
Chapter 10	Fabric OS FCIP Administrator’s Guide	
	In this chapter	25
	Documentation updates for Fabric OS v7.0.0 and later.	25
	Chapter 2, FCIP on the 7800 Switch and FX8-24 Blade.	25
Chapter 11	Fabric OS MIB Reference	
	In this chapter	27
	Documentation updates for Fabric OS v7.0.1.	27
	Chapter 1, Understanding Brocade SNMP.	27
	Chapter 4, FE MIB Objects	28
	Chapter 5, Entity MIB Objects	29
	Chapter 6, SW-MIB Objects.	29
	Chapter 7, High-Availability MIB Objects	30
	Chapter 9, FibreAlliance MIB Objects.	30
	Chapter 11, FCIP MIB Objects.	30
Chapter 12	Fabric OS Troubleshooting and Diagnostics Guide	
	In this chapter	33
	Documentation updates for Fabric OS v7.0.0 and later.	33
	Appendix A, Switch Type and Blade ID	33
	Documentation updates for Fabric OS v7.0.1 and later.	34
	Chapter 10, Diagnostic Features	34
	Appendix A, Switch Type and Blade ID	34
Chapter 13	Fabric Watch Administrator’s Guide	
	In this chapter	35
	Documentation updates for Fabric Watch v7.0.0 and later.	35
	Chapter 1. Fabric Watch	35
	Chapter 8. System Monitoring	35
	Chapter 9. Fabric Watch configuration using Web Tools.	36
Chapter 14	Web Tools Administrator’s Guide	
	In this chapter	37
	Documentation updates for Fabric OS v7.0.0.	37
	Chapter 9, Administering Zoning	37

	Documentation updates for Fabric OS v7.0.1.....	37
	About This Document	37
	Chapter 1, Introducing Web Tools.....	37
	Chapter 2, Using the Web Tools Interface	38
	Chapter 6, Managing Ports.....	38
	Chapter 11, Using the FC-FC Routing Service	38
	Chapter 14, Administering Extended Fabrics.....	39
	Chapter 15, Routing Traffic.....	39
	Chapter 17, Administering FICON CUP Fabrics	39
Chapter 15	Brocade 6510 Hardware Reference Manual	
	In this chapter	41
	Chapter 2, Brocade 6510 Installation and Configuration	41
	Appendix A, Brocade 6510 Specifications	41
Chapter 16	Brocade DCX 8510-8 Backbone Hardware Reference Manual	
	In this chapter	43
	Chapter 5, Removal and Replacement Procedures	43
	Preparing for the WWN card replacement.....	43
Chapter 17	Brocade DCX 8510-4 Hardware Reference Manual	
	In this chapter	45
	Chapter 5, Removal and Replacement Procedures	45
	Preparing for the WWN card replacement.....	45
Chapter 18	Brocade DCX Backbone Hardware Reference Manual	
	In this chapter	47
	Chapter 5, Removal and Replacement Procedures	47
	Preparing for the WWN card replacement.....	47
Chapter 19	Brocade DCX-4S Backbone Hardware Reference Manual	
	In this chapter	49
	Chapter 5, Removal and Replacement Procedures	49
	Preparing for the WWN card replacement.....	49

About This Document

In this chapter

- [How this document is organized](#) vii
- [What's new in this document](#) viii
- [Brocade Resources](#) ix
- [Document feedback](#) ix

How this document is organized

This document contains updates to the Fabric OS v7.0.x product manuals: These updates include document fixes and changes covering new features. [Table 1](#) below list the most recently released Fabric OS v7.0.x product manuals.

TABLE 1 Documentation Supporting Fabric OS v7.0.x

Publication Title	Fabric OS Release	Page Number	Publication Date
<i>Access Gateway Administrator's Guide</i>	v7.0.0 and later	Updates on page 1	April 2011
<i>Converged Enhanced Ethernet Administrator's Guide</i>	v7.0.0 and later	No Updates	April 2011
<i>Converged Enhanced Ethernet Command Reference</i>	v7.0.0 and later	Updates on page 3	August 2011
<i>Fabric OS Administrator's Guide</i>	v7.0.0 and later v7.0.1 and later	Updates on page 5 Updates on page 6	July 2011 December 2011
<i>Fabric OS Command Reference</i>	v7.0.0 v7.0.1	Updates on page 9 Updates on page 7	April 2011 December 2011
<i>Fabric OS Encryption Administrator's Guide (LKM)</i>	v7.0.0 and later	Updates on page 13	June 2011
<i>Fabric OS Encryption Administrator's Guide (RKM)</i>	v7.0.0 and later	Updates on page 15	June 2011
<i>Fabric OS Encryption Administrator's Guide (SKM)</i>	v7.0.0 and later	Updates on page 19	July 2011
<i>Fabric OS Encryption Administrator's Guide (TEMS)</i>	v7.0.0 and later	Updates on page 21	June 2011
<i>Fabric OS Encryption Administrator's Guide (TKLM)</i>	v7.0.0 and later	Updates on page 23	June 2011
<i>Fabric OS FCIP Administrator's Guide</i>	v7.0.0 and later	Updates on page 25	April 2011
<i>Fabric OS Message Reference</i>	v7.0.0 and later	No Updates	April 2011
<i>Fabric OS MIB Reference</i>	v7.0.0 v7.0.1	No Updates Update on page 27	April 2011 December 2011
<i>Fabric OS Troubleshooting and Diagnostics Guide</i>	v7.0.0 and later	Update on page 33	June 2011
<i>Fabric Watch Administrator's Guide</i>	v7.0.0 and later	Update on page 35	April 2011
<i>FICON Administrator's Guide</i>	v7.0.0 and later	No Updates	April 2011

TABLE 1 Documentation Supporting Fabric OS v7.0.x (Continued)

Publication Title	Fabric OS Release	Page Number	Publication Date
<i>Web Tools Administrator's Guide</i>	v7.0.0	Updates on page 37	April 2011
	v7.0.1	Updates on page 37	December 2011
<i>6510 Hardware Reference Manual</i>	v7.0.0 and later	Updates on page 41	August 2011
<i>DCX 8510-8 Backbone Hardware Reference Manual</i>	v7.0.0 and later	Updates on page 43	July 2011
<i>DCX 8510-4 Backbone Hardware Reference Manual</i>	v7.0.0 and later	Updates on page 45	July 2011
<i>DCX Backbone Hardware Reference Manual</i>	v7.0.0 and later	Updates on page 47	March 2010
<i>DCX-4S Backbone Hardware Reference Manual</i>	v7.0.0 and later	Updates on page 49	June 2010

What's new in this document

The following changes have been made since this document was last released:

- Updates for the Fabric OS Administrator's Guide have been added for the 7.0.1 release, to correct the table "Configurable distances for Extended Fabrics". Also, corrections were made to the updates for the 7.0.0 release regarding this same table.
- Documentation updates for Fabric OS v7.0.1 have been added to the [Fabric OS Command Reference](#) chapter. The following command help pages have been updated or corrected:
 - [portCfgDPort](#)
 - [portCfgShow](#)
 - [portStatsShow](#)
 - [rtLogTrace](#)
- Chapter for the *Fabric OS MIB Reference* has been added to include the 7.0.1 release updates.
- Updates for the *Fabric OS Troubleshooting and Diagnostics Guide* have been added, for both the Fabric OS v7.0.0 release and for the v7.0.1 release.
- The *Web Tools Administrator's Guide* has been updated to include the 7.0.1 release updates.
- Chapters have been added for the following Hardware Reference Manuals:
 - Brocade 6510
Several small changes for "Local time synchronization," "Setting the date," both in "[Chapter 2, Brocade 6510 Installation and Configuration](#)," and the "General specifications" table in "[Appendix A, Brocade 6510 Specifications](#)."
 - Brocade DCX 8510-8 Backbone
Significant changes to the "WWN card removal and replacement" procedure in "[Chapter 5, Removal and Replacement Procedures](#)."
 - Brocade DCX 8510-4 Backbone
Significant changes to the "WWN card removal and replacement" procedure in "[Chapter 5, Removal and Replacement Procedures](#)."
 - Brocade DCX Backbone
Significant changes to the "Removal and replacement of WWN card" procedure in "[Chapter 5, Removal and Replacement Procedures](#)."
 - Brocade DCX-4S Backbone
Significant changes to the "Removal and replacement of WWN card" procedure in "[Chapter 5, Removal and Replacement Procedures](#)."

Brocade Resources

To get up-to-the-minute information, go to <http://my.brocade.com> and register at no cost for a user ID and password.

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

<http://www.amazon.com>

For additional Brocade documentation, visit the Brocade SAN Info Center and click the Resource Library location:

<http://www.brocade.com>

Release notes are available on the MyBrocade web site and are also bundled with the Fabric OS firmware.

Document feedback

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. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Access Gateway Administrator's Guide

In this chapter

The updates in this chapter are for the *Access Gateway Administrator's Guide*, publication number 53-1002156-01, published April 2011.

- [Documentation updates for Fabric OS v7.0.0 and later](#) 1

Documentation updates for Fabric OS v7.0.0 and later

Chapter 2, Configuring Ports in Access Gateway Mode

Under the heading of “Default port mapping” on page 11, the following note has changed to include the Brocade 6510:

NOTE

All ports on demand (POD) licenses must be present to use Access Gateway on the Brocade 5100, 300, and 6510.

1 Documentation updates for Fabric OS v7.0.0 and later

CEE Command Reference

In this chapter

The updates in this chapter are for the *Converged Enhanced Ethernet Command Reference*, publication number 53-1002164-01, published April 2011.

- [Documentation updates for Fabric OS v7.0.0 and later](#) 3

Documentation updates for Fabric OS v7.0.0 and later

Under the command **show statistics access-list mac**, replace the Command Modes entry with the following:

Command Modes	Privileged EXEC mode
----------------------	----------------------

Under the command **show mac-address-table**, replace the Command Modes entry with the following:

Command Modes	Privileged EXEC mode
----------------------	----------------------

show running-config

Displays the contents of the configuration file currently running on the system.

Synopsis	show running-config { access-list cee-map dot1x interface linecard lldp rmon spanning-tree }																
Operands	<table border="0"> <tr> <td style="padding-right: 20px;">access-list</td> <td>Displays the running configuration of the access list.</td> </tr> <tr> <td>cee-map</td> <td>Displays the QoS Converged Enhanced Ethernet (CEE) maps configuration.</td> </tr> <tr> <td>dot1x</td> <td>Displays the 802.1X Port-Based Access Control configuration.</td> </tr> <tr> <td>interface</td> <td>Displays the interface configuration.</td> </tr> <tr> <td>linecard</td> <td>Displays the linecard configuration.</td> </tr> <tr> <td>lldp</td> <td>Displays the LLDP configuration.</td> </tr> <tr> <td>rmon</td> <td>Displays the Remote Monitoring Protocol (RMON) configuration.</td> </tr> <tr> <td>spanning-tree</td> <td>Displays the STP switch configuration.</td> </tr> </table>	access-list	Displays the running configuration of the access list.	cee-map	Displays the QoS Converged Enhanced Ethernet (CEE) maps configuration.	dot1x	Displays the 802.1X Port-Based Access Control configuration.	interface	Displays the interface configuration.	linecard	Displays the linecard configuration.	lldp	Displays the LLDP configuration.	rmon	Displays the Remote Monitoring Protocol (RMON) configuration.	spanning-tree	Displays the STP switch configuration.
access-list	Displays the running configuration of the access list.																
cee-map	Displays the QoS Converged Enhanced Ethernet (CEE) maps configuration.																
dot1x	Displays the 802.1X Port-Based Access Control configuration.																
interface	Displays the interface configuration.																
linecard	Displays the linecard configuration.																
lldp	Displays the LLDP configuration.																
rmon	Displays the Remote Monitoring Protocol (RMON) configuration.																
spanning-tree	Displays the STP switch configuration.																
Defaults	There are no default configurations for this command.																
Command Modes	Privileged EXEC mode EXEC mode																
Description	Use this command to display the contents of the configuration file currently running on the system. The show running-config command displays only the commands that were successfully executed.																
Usage Guidelines	There are no usage guidelines for this command.																
Examples	<p>To display the content of the current configuration file:</p> <pre>switch#show running-config ! no protocol spanning-tree ! interface Vlan 1 ! interface TenGigabitEthernet 0/0 shutdown ! interface TenGigabitEthernet 0/1 shutdown ! interface TenGigabitEthernet 0/2 shutdown ! interface TenGigabitEthernet 0/3 shutdown ! interface TenGigabitEthernet 0/4 shutdown</pre>																
See Also	show startup-config																

Fabric OS Administrator's Guide

In this chapter

- Documentation updates for Fabric OS v7.0.0 and later 5
- Documentation updates for Fabric OS v7.0.1 and later 6

Documentation updates for Fabric OS v7.0.0 and later

The updates in this section are for the *Fabric OS Administrator's Guide*, publication number 53-1002148-03, published July 2011.

Chapter 22, Managing Long Distance Fabrics

Under the heading of “Configuring an extended ISL” on page 451, in step 3, change the default value of R_A_TOV from 1000 to 10000.

Under the heading of “Buffer credits for each switch model” on page 458, change the first paragraph to the following:

Table 78 shows the total ports in a switch or blade, number of user ports in a port group, and the unreserved buffer credits available per port group. The number in the **Unreserved buffers** column is the number with QoS enabled. This number is higher if QoS is not enabled.

In Table 78, “Buffer credits” on page 458, change the name of the last column to “**Unreserved buffers (per port group) with QoS enabled**”.

In Table 79, “Configurable distances for Extended Fabrics” on page 460, change the values for the Brocade 6510, FC16-32, and FC16-48 to the following:

TABLE 79 Configurable distances for Extended Fabrics

Switch/blade model	Maximum distances (km) that can be configured assuming 2112 Byte Frame Size					
	1 Gbps	2 Gbps	4 Gbps	8 Gbps	10 Gbps	16 Gbps
6510	N/A	6754	3377	1688	1350	844
FC16-32	N/A	5190	2595	1297	1038	648
FC16-48	N/A	4486	2243	1121	897	560

On page 460, change the note after Table 79 from this:

NOTE
QoS requires an additional 20 buffer credits per active port so maximum supported distances may be lower.

To this:

NOTE
The distances in Table 79 assume QoS is enabled. If QoS is disabled, the maximum supported distances are higher because QoS requires an additional 20 buffer credits per active port.

Documentation updates for Fabric OS v7.0.1 and later

The updates in this section are for the *Fabric OS Administrator's Guide*, publication number 53-1002446-01, published December 2011.

Chapter 23, Managing Long Distance Fabrics

In Table 80, "Configurable distances for Extended Fabrics" on page 462, change the values for the Brocade 6505, 6510, FC8-32E, FC8-48E, FC16-32, and FC16-48 to the following:

TABLE 80 Configurable distances for Extended Fabrics

Maximum distances (km) that can be configured assuming 2112 Byte Frame Size						
Switch/blade model	1 Gbps	2 Gbps	4 Gbps	8 Gbps	10 Gbps	16 Gbps
6505	N/A	7426	3713	1856	1485	928
6510	N/A	6754	3377	1688	1350	844
FC8-32E	N/A	5190	2595	1297	1038	648
FC8-48E	N/A	4486	2243	1121	897	560
FC16-32	N/A	5190	2595	1297	1038	648
FC16-48	N/A	4486	2243	1121	897	560

On page 462, change the note at the bottom of the page from this:

NOTE
QoS requires an additional 20 buffer credits per active port so maximum supported distances may be lower.

To this:

NOTE
The distances in Table 80 assume QoS is enabled. If QoS is disabled, the maximum supported distances are higher because QoS requires an additional 20 buffer credits per active port.

Fabric OS Command Reference

In this chapter

- [Documentation Updates for Fabric OS v7.0.1](#) 7
- [Documentation Updates for Fabric OS v7.0.0](#) 9

Documentation Updates for Fabric OS v7.0.1

The updates in this section are for the *Fabric OS Command Reference*, publication number 53-1002447-01, published December 15, 2011.

The note on page xxi in the Preface includes an incorrect platform reference. The note should read:

portCfgOctetSpeedCombo - Not supported on the Brocade 6505; supported on the Brocade FC8-32E and FC8-48E port blades only with the default combination.

portCfgDPort

Add the following configuration option to the portCfgDport --enable command:

portcfgdport --enable [slot/]port_list **dwdm**

Skips the optical loopback test when you run the D_Port diagnostics over a Dense Wavelength Division Multiplexing (DWDM) link or any third party equipment that connects two switches.

D_Port functionality is only available on 16Gbit-capable platforms with 16Gb SFPs and 10Gb FC SFPs.

portCfgShow

On page 688, add the following descriptions under the "Non-GbE port displays" section:

Octet Speed Combo: Displays the current octet speed combo setting. This parameter is set by the **portCfgOctetSpeed** command. In unsupported platforms, this display is not shown

D-Port over DWDM Displays ON when the D_Port is configured over a DWDM link. This parameter is set by portCfgDPort command and displays only if portCfgDPort is configured with the **dwdm** option.

portStatsShow

This command has been updated to include the following counters. These counters are supported only on Condor3-based platforms and display only on these platforms

er_single_credit_loss

Displays the number of times that the port lost single VC_RDY primitive signal or a single frame.

er_multi_credit_loss

Displays the number of times that the port lost multiple VC_RDY primitive signals or multiple frames

To display the port statistics on the Brocade 5610:

```
switch:admin> portstatshow 0
stat_wtx          635621      4-byte words transmitted
stat_wrx          386290      4-byte words received
stat_ftx          31573       Frames transmitted
stat_frx          27373       Frames received
stat_c2_frx       0          Class 2 frames received
stat_c3_frx       0          Class 3 frames received
stat_lc_rx        13678      Link control frames received
stat_mc_rx        0          Multicast frames received
stat_mc_to        0          Multicast timeouts
stat_mc_tx        0          Multicast frames transmitted
tim_rdy_pri       0          Time R_RDY high priority
tim_txcrd_z       62084      Time TX Credit Zero (2.5Us ticks)
tim_txcrd_z_vc 0- 3: 62084      0          0          0
tim_txcrd_z_vc 4- 7: 0          0          0          0
tim_txcrd_z_vc 8-11: 0          0          0          0
tim_txcrd_z_vc 12-15: 0          0          0          0
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        8336      Encoding error outside of frames
er_enc_pcs_err    0          pcs error
er_bad_os         6          Invalid ordered set
er_rx_c3_timeout 0          Class 3 receive frames discarded due to timeout
er_tx_c3_timeout 0          Class 3 transmit frames discarded due to
timeout
er_unroutable     17         Frames that are unroutable
er_unreachable    0          Frames with unreachable destination
er_other_discard  0          Other discards
er_type1_miss     0          frames with FTB type 1 miss
er_type2_miss     0          frames with FTB type 2 miss
er_type6_miss     0          frames with FTB type 6 miss
er_zone_miss      0          frames with hard zoning miss
er_lun_zone_miss  0          frames with LUN zoning miss
er_crc_good_eof   0          Crc error with good eof
er_inv_arb        0          Invalid ARB
er_single_credit_loss 0          Single vcrdy/frame loss on link
er_multi_credit_loss 0          Multiple vcrdy/frame loss on link
```

rtLogTrace

The statement on page 877 regarding the persistence of the **rtLogTrance** configuration is incorrect. It should read: "The RTLog is enabled by default and persistent across reboots. The **rtLogTrace** configuration is lost after a power cycle."

Correct the description of the enable option as follows:

--enable Enables the RTLog on the active Control Processor (CP). The RTLog becomes effective on the standby CP after a failover or a reboot of the *active CP*.

Documentation Updates for Fabric OS v7.0.0

The updates in this section are for the *Fabric OS Command Reference*, publication number 53-1002147-01, published April 2011.

bottleneckMon

On page 74, add the error message ID (RAS Cx-1018) to the description of the credit recovery feature as shown:

When used with the **-recover onLrThresh** option, recovery is attempted through repeated link resets and a count of the link resets is kept. If the threshold of more than two link resets per hour is reached, the blade is faulted (RAS Cx-1018). Note that regardless of whether the link reset occurs on the port blade or on the core blade, the port blade is always faulted.

configure

The **configure** command was accidentally omitted from the “Modified Commands” section in the Preface. The command was modified to add the Enforced FLOGI/FDISC login parameter.

configureChassis

Add the following note to the **configureChassis** command: All configuration changes made by this command are non-disruptive. It is not necessary to disable the switch.

On page 151, and in the associated manual page, replace the description of the *system.i2cTurboCnfg* parameter with the following text:

system.i2cTurboCnfg *value*

Configures the i2c driver that manages processing of the i2c interrupts. The I2CTurbo mode is enabled (Setting 1) by default on all 16G platforms running Fabric OS v7.0 firmware. The mode is disabled by default for any switches capable of running v6.4x and v6.3x firmware. An upgrade preserves the pre-upgrade configuration. The value shown in square brackets is the current value. The following values are supported:

- 0 Disables the I2C Turbo mode. When the I2C Turbo mode is disabled, every byte received by an i2c interrupt is scheduled for processing by the given task or process. This permits other high priority processes to complete, thereby allowing for possible delay in the receipt of the I2C response message.
- 1 Enables the I2C turbo mode for SFPs. This is the default setting. When the I2C Turbo mode is enabled, every I2C byte received from an SFP is processed by the interrupt handler itself, thus preventing any higher priority processes from preempting this processing.
- 2 For internal use only.

cryptoCfg

On page 159, modify the description of the **cryptocfg -reg -KAClogin** parameter as shown and add the example in the example section:

--reg -KAClogin Registers the node KAC login credentials (username and password) with the configured key vaults. This command is valid for the Thales nCipher (TEMS), the HP SKM, and the TKLM key vaults. This command must be run on each member node. For key vault configuration procedures, refer to the Fabric OS Encryption Administrator's Guide for your specific key vault product.

On page 165, add the TKLM key vault to the set of key vaults displayed by the **--show groupcfg** command.

The NCKA key vault is now referred to as TEMS and should be updated in all places where the NCKA key vault is mentioned.

Use the **--show -groupcfg** command to display encryption group and member configuration parameters, including the following parameters:

- Encryption group name: user-defined label
- Encryption group policies:
 - Failback mode: Auto or Manual
 - Replication mode: Enabled or Disabled
 - Heartbeat misses: numeric value
 - Heartbeat timeout: value in seconds
 - Key Vault Type: LKM, RKM, SKM, **TEMS, or TKLM**.
 - System Card: Disabled or Enabled
- For each configured key vault, primary and secondary, the command shows:
 - IP address: The key vault IP address
 - Certificate ID: the key vault certificate name
 - State: connected, disconnected, up, authentication failure, or unknown.
 - Type: LKM, RKM, SKM, **TEMS, or TKLM**

On Page 173, replace the example for exporting the master key with the example shown:

To export the master key to the RKM key vault:

```
SecurityAdmin:switch> cryptocfg --exportmasterkey
Enter passphrase:*****

Confirm passphrase:*****

Master key exported.
Master Key ID: 11:95:82:cd:80:88:41:31:42:dd:c3:5f:d0:a7:95:55
Exported Key ID: 11:95:82:cd:80:88:41:31:42:dd:c3:5f:d0:a7:95:56
```

fruReplace

This command is no longer supported as of Fabric OS v7.0.0. Refer to the *WWN Card Remove and Replace Procedure (53-1000832-05)* for information on how to replace a WWN card without this command.

portLoopBackTest

Augment the note on page 751 and in the corresponding man pag as followse:

This diagnostic cannot be run on an operational switch. You must disable the switch using the **chassisDisable** command before you can run this test. After the test completes, re-enable the switch using the **chassisEnable** command.

Do NOT use the **switchDisable** command followed by manually shutting down the ports before running the test. This will not work, because executing **switchEnable**, after the test completes, will leave the ports in the same state as before. The only way to bring the ports down before running the test and back up after the test completes is by using the **chassisDisable** command followed by the **chassisEnable** command

turboRamTest

:Augment the note section of the **turboRamTest** help pages as followse:

This diagnostic cannot be run on an operational switch. You must disable the switch using the **chassisDisable** command before you can run this test. After the test completes, re-enable the switch using the **chassisEnable** command.

portLedTest

:Augment the note section of the **portLedtestTest** help pages as followse:

This diagnostic cannot be run on an operational switch. You must disable the switch using the **chassisDisable** command before you can run this test. After the test completes, re-enable the switch using the **chassisEnable** command.

slotShow

In the Notes section, the following note to clarify the description of slot 5 in a DCX and in a DCX-4S.

In a DCX-4S, slot 5 is occupied by a control processor blade (Blade ID 50). On a DCX, slot 5 is occupied by the core blade (Blade ID 52).

On page 927, the description for the **-p** operand should be clarified to avoid the impression that this command displays real-time power consumption data. This is not the case. Real-time power consumption data is displayed for 16G platforms only with the **chassisShow** command. The data displayed in the "DC Power Consumption" column and in the summary field "Total DC Power consumption" indicate the maximum allowed power consumption, not a real-time value.

- p** In addition to the basic slot status view, this command displays the following information about power consumption:
- The maximum allowed direct current (DC) power consumption for the chassis and individual values for each blade (in Watts). Note that usage for other components is included but not listed

4 supportSave

supportSave

Add the following note to the **supportSave** command and associated man page:

If you use anonymous FTP to run **supportSave** on a chassis with multiple AP blades, configure the FTP windows server to allow unlimited anonymous users.

Fabric OS Encryption Guide Supporting LKM

In this chapter

The updates in this chapter are for the *Fabric OS Encryption Administrator's Guide Supporting NetApp Lifetime Key Manager (LKM) Environments*, publication number 53-1002160-02, published June 2011.

Documentation updates for LKM

Chapter 3, Configuring Brocade Encryption Using CLI

Failover/failback policy configuration

A correction has been made to heartbeat values for the following:

- Heartbeat misses—The range is 3-14 in integer increments only.
- Heartbeat timeout—The range is 2-9 seconds in integer increments only.

Chapter 5, Best Practices and Special Topics

Key Vault Best Practices

When encrypted disk LUNs are to be configured or moved to an Encryption Group that uses a different key vault, make sure to decommission the encrypted LUNs from the old Encryption Group.

Chapter 6, Maintenance and Troubleshooting

Manually synchronizing the security database

This operation can resolve problems with master key propagation (and connectivity issues between peer node encryption engines in an encryption group). The synchronization occurs every time this command is executed regardless of whether or not the security database was synchronized across all nodes in the encryption group.

Use the `-sync -securitydb` command to distribute the security database from the group leader node to all member nodes. This command is valid only on the group leader.

In scenarios where this master key propagation issue still persists, exporting the master key to a file and recovering it resolves the issue. To do this, use the following commands:

5 Documentation updates for LKM

- Use the `cryptocfg --exportmasterkey -file` option to export the master key to a file.
- Use the `cryptocfg --recovermasterkey currentMK -srcfile` to recover the master key.

Fabric OS Encryption Guide Supporting RKM

In this chapter

The updates in this chapter are for the *Fabric OS Encryption Administrator's Guide Supporting RSA Key Manager (RKM) Environments*, publication number 53-1002158-02, published June 2011.

Documentation updates for RKM

Chapter 2, Encryption configuration using the Management application

Disk device decommissioning

Under the heading of “Displaying and deleting decommissioned key IDs” on page 87, additional steps in the procedure have been added that must be performed from the RKM key vault server.

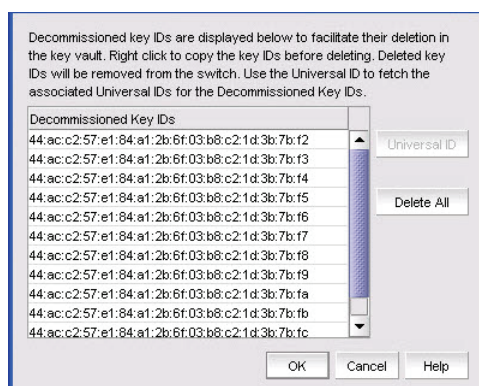


FIGURE 1 Decommissioned Key IDs dialog box

When disk LUNs are decommissioned, the process includes the disabling of the key record in the key vault and indication that the key has been decommissioned. These decommissioned key IDs are still stored on the switch. You can display, copy, and delete them as an additional security measure.

For RKM key vaults, you need to know the Universal ID (UUID) associated with the decommissioned LUN key IDs to delete keys from the key vault. To delete decommissioned key IDs, you must first display the vendor-specific UUIDs of decommissioned key IDs for RKM key vaults from the Management application. You must then remove key attributes directly from the RKM key vault server.

1. Select **Configure > Encryption** from the menu task bar.

The **Encryption Center** dialog box displays.

2. Select a switch from the **Encryption Center Devices** table, then select **Switch > Decommissioned key IDs** from the menu task bar, or right-click a switch and select **Decommissioned key IDs**.

The **Decommissioned Key IDs** dialog box displays.

3. Click **Delete All** to delete the decommissioned key IDs from the switch. As a precaution, you might want to copy the key IDs to a secure location before deleting them from the switch. To export the key IDs, right-click and select **Export**, which will export the key IDs.

NOTE

Select the desired decommissioned key IDs from the Management application **Decommissioned Key IDs** table, then click **Universal ID**. The **Universal IDs** dialog box displays.

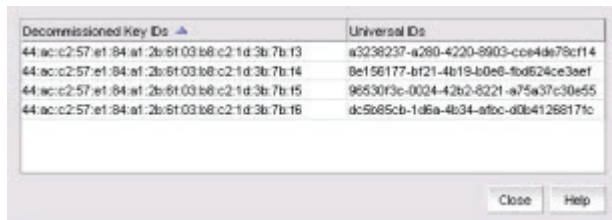


FIGURE 2 Universal IDs dialog box

4. Log in to the RKM key vault.
3. Click **Key Classes**.
 - a. Click **view option** for “**Key Class: kcn.1998-01.com.brocade:DEK_AES_256_XTS**”
 - b. On filters, select **UUID**, then copy and paste the UUID value of the decommissioned key.
 - c. Click **Apply**.

The key details are displayed.

5. Deactivate and destroy the key.
6. Click the MUID link to get the key attribute details for the key.
7. Under **Key Object Attributes**, remove the following attributes, then click **Update**.
 - **Keyid**
 - **Keystate**
 - **Media id**
 - **Media type**

Chapter 3, Configuring Brocade Encryption Using CLI

Failover/failback policy configuration

A correction has been made to heartbeat values for the following:

- Heartbeat misses—The range is 3-14 in integer increments only.
- Heartbeat timeout—The range is 2-9 seconds in integer increments only.

Chapter 5, Best Practices and Special Topics

Key Vault Best Practices

- When encrypted disk LUNs are to be configured or moved to an Encryption Group that uses a different key vault, make sure to decommission the encrypted LUNs from the old Encryption Group.

Chapter 6, Maintenance and Troubleshooting

Manually synchronizing the security database

This operation can resolve problems with master key propagation (and connectivity issues between peer node encryption engines in an encryption group). The synchronization occurs every time this command is executed regardless of whether or not the security database was synchronized across all nodes in the encryption group.

Use the `-sync -securitydb` command to distribute the security database from the group leader node to all member nodes. This command is valid only on the group leader.

In scenarios where this master key propagation issue still persists, exporting the master key to a file and recovering it resolves the issue. To do this, use the following commands:

- Use the `cryptocfg --exportmasterkey -file` option to export the master key to a file.
- Use the `cryptocfg --recovermasterkey currentMK -srcfile` to recover the master key.

6 Documentation updates for RKM

Fabric OS Encryption Guide Supporting SKM and ESKM

In this chapter

The updates in this chapter are for the *Fabric OS Encryption Administrator's Guide Supporting HP Secure Key Manager (SKM) Environments*, and *HP Enterprise Secure Key Manager (ESKM) Environments* publication number 53-1002159-03, published July 2011.

Documentation updates for SKM

Chapter 3, Configuring Brocade Encryption Using CLI

Failover/failback policy configuration

A correction has been made to heartbeat values for the following:

- Heartbeat misses—The range is 3-14 in integer increments only.
- Heartbeat timeout—The range is 2-9 seconds in integer increments only.

Chapter 5, Best Practices and Special Topics

Key Vault Best Practices

When encrypted disk LUNs are to be configured or moved to an Encryption Group that uses a different key vault, make sure to decommission the encrypted LUNs from the old Encryption Group.

Chapter 6, Maintenance and Troubleshooting

Manually synchronizing the security database

This operation can resolve problems with master key propagation (and connectivity issues between peer node encryption engines in an encryption group). The synchronization occurs every time this command is executed regardless of whether or not the security database was synchronized across all nodes in the encryption group.

Use the `-sync -securitydb` command to distribute the security database from the group leader node to all member nodes. This command is valid only on the group leader.

In scenarios where this master key propagation issue still persists, exporting the master key to a file and recovering it resolves the issue. To do this, use the following commands:

7 Documentation updates for SKM

- Use the `cryptocfg --exportmasterkey -file` option to export the master key to a file.
- Use the `cryptocfg --recovermasterkey currentMK -srcfile` to recover the master key.

Fabric OS Encryption Guide Supporting TEMS

In this chapter

The updates in this chapter are for the *Fabric OS Encryption Administrator's Guide Supporting Thales Encryption Manager for Storage (TEMS) Environments*, publication number 53-1002161-02, published June 2011.

Documentation updates for TEMS

Chapter 3, Configuring Brocade Encryption Using CLI

Failover/failback policy configuration

A correction has been made to heartbeat values for the following:

- Heartbeat misses—The range is 3-14 in integer increments only.
- Heartbeat timeout—The range is 2-9 seconds in integer increments only.

Chapter 5, Best Practices and Special Topics

Key Vault Best Practices

When encrypted disk LUNs are to be configured or moved to an Encryption Group that uses a different key vault, make sure to decommission the encrypted LUNs from the old Encryption Group.

Chapter 6, Maintenance and Troubleshooting

Manually synchronizing the security database

This operation can resolve problems with master key propagation (and connectivity issues between peer node encryption engines in an encryption group). The synchronization occurs every time this command is executed regardless of whether or not the security database was synchronized across all nodes in the encryption group.

Use the `-sync -securitydb` command to distribute the security database from the group leader node to all member nodes. This command is valid only on the group leader.

In scenarios where this master key propagation issue still persists, exporting the master key to a file and recovering it resolves the issue. To do this, use the following commands:

8 Documentation updates for TEMS

- Use the `cryptocfg --exportmasterkey -file` option to export the master key to a file.
- Use the `cryptocfg --recovermasterkey currentMK -srcfile` to recover the master key.

Fabric OS Encryption Guide Supporting TEMS

In this chapter

The updates in this chapter are for the *Fabric OS Encryption Administrator's Guide Supporting Tivoli Key Lifecycle Manager (TKLM) Environments*, publication number 53-1002162-02, published June 2011.

Documentation updates for TKLM

Chapter 3, Configuring Brocade Encryption Using CLI

Failover/failback policy configuration

A correction has been made to heartbeat values for the following:

- Heartbeat misses—The range is 3-14 in integer increments only.
- Heartbeat timeout—The range is 2-9 seconds in integer increments only.

Chapter 5, Best Practices and Special Topics

Key Vault Best Practices

When encrypted disk LUNs are to be configured or moved to an Encryption Group that uses a different key vault, make sure to decommission the encrypted LUNs from the old Encryption Group.

Chapter 6, Maintenance and Troubleshooting

Manually synchronizing the security database

This operation can resolve problems with master key propagation (and connectivity issues between peer node encryption engines in an encryption group). The synchronization occurs every time this command is executed regardless of whether or not the security database was synchronized across all nodes in the encryption group.

Use the `-sync -securitydb` command to distribute the security database from the group leader node to all member nodes. This command is valid only on the group leader.

In scenarios where this master key propagation issue still persists, exporting the master key to a file and recovering it resolves the issue. To do this, use the following commands:

9 Documentation updates for TKLM

- Use the `cryptocfg --exportmasterkey -file` option to export the master key to a file.
- Use the `cryptocfg --recovermasterkey currentMK -srcfile` to recover the master key.

Fabric OS FCIP Administrator's Guide

In this chapter

The updates in this chapter are for the *Fabric OS FCIP Administrator's Guide*, publication number 53-1002155-01, published April 2011.

- [Documentation updates for Fabric OS v7.0.0 and later](#) 25

Documentation updates for Fabric OS v7.0.0 and later

Chapter 2, FCIP on the 7800 Switch and FX8-24 Blade

Under the heading of “7800 switch license options” on page 6, change the following bullet item since a 7800 upgrade license is not required to enable the Advanced FICON Acceleration License on the 7800 switch.

- The 7800 upgrade license to enable full hardware capabilities, full FCIP tunnel capabilities, support of advanced capabilities, such as Open Systems Tape Pipelining (OSTP), and FICON CUP support.

In Table 2, “7800 FCIP feature licenses,” on page 7, change the following information since a 7800 upgrade license is not required to enable the Advanced FICON Acceleration License on the 7800 switch.

TABLE 2 7800 FCIP feature licenses

Feature	Purpose	License (licenseShow output)
7800 upgrade	Enables full hardware capabilities, full FCIP tunnel capabilities, support of advanced capabilities like open systems tape pipelining (OSTP), and FICON CUP support.	7800 Upgrade license

10 Documentation updates for Fabric OS v7.0.0 and later

Fabric OS MIB Reference

In this chapter

The updates in this chapter are for the *Fabric OS MIB Reference*, part number: 53-1002151-01, published April 2011.

- [Documentation updates for Fabric OS v7.0.1](#) 27

Documentation updates for Fabric OS v7.0.1

Chapter 1, Understanding Brocade SNMP

Under the heading “Before Loading MIBs” on page 9, add the following row to Table 2.

TABLE 2 Fabric OS-supported SNMP versions

Firmware	SNMPv1	SNMPv2	SNMPv3
Fabric OS v7.0.1	Yes	No	Yes

Under the heading “SNMP CLI usage” on page 19, change the note to the following:

NOTE

SNMPv3 supports AES128 and DES protocols. SNMPv3 does not support privacy protocols AES192, AES256, and 3DES.

11 Documentation updates for Fabric OS v7.0.1

Chapter 4, FE MIB Objects

Under the heading “Definitions for FIBRE-CHANNEL-FE-MIB” on page 75, replace the following rows in Table 9.

TABLE 9 FIBRE-CHANNEL-FE-MIB definitions

Type Definition	Value	Description
FcFeFxPortCapacity	Integer from 1 to 640	Maximum number of Fx_Ports within a module. For the Brocade 300, this value is 24. For the Brocade 4100, this value is 32. For the Brocade 4900, this value is 64. For the Brocade 5000, this value is 32. For the Brocade 5100, this value is 40. For the Brocade 5300, this value is 80. For the Brocade 7500 or 7500E, this value is 32. For the Brocade 7600, this value is 16. For the Brocade 7800 Extension Switch, this value is 24. For the Brocade 8000, this value is 32. For the Brocade Encryption switch, this value is 32. For the Brocade DCX, this value is 640. For the Brocade DCX-4S, this value is 320. For the Brocade 48000, this value is 384. For the Brocade 6510, this value is 48. For the Brocade DCX 8510-4 Backbone, this value is 320. For the Brocade DCX 8510-8 Backbone, this value is 640. For the Brocade 6505, this value is 24. For the Brocade VA-40FC, this value is 40.
fcfeModuleFxPortCapacity	Integer from 1 to 640	Maximum number of Fx_Ports within a module.

Under the MIB object “fcFeModuleFxPortCapacity 1.3.6.1.2.1.75.1.1.4.1.6” on page 77, add the following to the existing list:

- Brocade 6505 24 ports
- Brocade VA-40FC 40 ports

Under the MIB object “entPhysicalClass 1.3.6.1.2.1.47.1.1.1.1.5” on page 109, add the following information:

Brocade 6505 switch can have the following hierarchy of physical objects:

- Chassis: One entry (one row)
- Container: One entry for each FRU slot (one switch blade, two power supplies, two fans)
- Module: One entry for switch blade, up to two entries for power supplies, and up to two entries for fans.

Brocade VA-40FC switch can have the following hierarchy of physical objects:

- Chassis: One entry (one row)
- Container: One entry for each FRU slot (one blade, two power supplies, two fans)
- Module: One entry for blades, two entries for power supplies, and two entries for fans

Chapter 5, Entity MIB Objects

Add the following rows to Table 13 on page 113.

TABLE 13 entPhysicalTable entries for Brocade switches

Platform	Blades	Fans	Power supply	WWN card
Brocade 6505	1	2 fans	2 PS	1 WWN unit. Not a FRU.
Brocade VA-40FC	1	2 fans	2 PS	1 WWN unit. Not a FRU.

Replace the following columns in Table 13 on page 113.

TABLE 13 entPhysicalTable entries for Brocade switches

Platform	WWN card
Brocade 6510	1 WWN unit. Not a FRU.
Brocade 8000	1 WWN unit. Not a FRU.
Brocade 7800 Extension Switch	1 WWN unit. Not a FRU.

Chapter 6, SW-MIB Objects

Add the following rows to Table 16 on page 145.

TABLE 16 Sensors on the various Brocade switches

Platform	Temp	Fans	Power supply	swNumSensors / connUnitNumSensors
Brocade 6505	4 sensors	2 fans	2 PS	8
Brocade VA-40FC	4 sensors	2 fans	2 PS	8

Add the following rows to Table 17 on page 145.

TABLE 17 Blade table

Model	Temp sensors
FC8-32E	7 sensors
FC8-48E	7 sensors

Under the MIB object “swFCPortCapacity 1.3.6.1.4.1.1588.2.1.1.1.6.1” on page 150, add the following to the existing list:

- Brocade 6505 24 ports
- Brocade VA-40FC 40 ports

Add the following note to the MIB objects listed in [Table 1](#).

NOTE

This object is deprecated.

11 Documentation updates for Fabric OS v7.0.1

TABLE 1 Deprecated MIB objects

Object	OID	On page
swFwLastEvent	1.3.6.1.4.1.1588.2.1.1.1.10.3.1.6	161
swFwLastEventVal	1.3.6.1.4.1.1588.2.1.1.1.10.3.1.7	161
swFwLastEventTime	1.3.6.1.4.1.1588.2.1.1.1.10.3.1.8	162
swFwBehaviorType	1.3.6.1.4.1.1588.2.1.1.1.10.3.1.10	162
swFwBehaviorInt	1.3.6.1.4.1.1588.2.1.1.1.10.3.1.11	162
swFwLastSeverityLevel	1.3.6.1.4.1.1588.2.1.1.1.10.3.1.12	162

Chapter 7, High-Availability MIB Objects

Add the following row to Table 20 on page 179.

TABLE 20 Valid FRU counts for the various Brocade switches

Platform	Blades	Fans	Power Supply	WWN Card
Brocade 6505	1	2 fans	2 PS	1 WWN

Chapter 9, FibreAlliance MIB Objects

Under the MIB object “connUnitNumports 1.3.6.1.3.94.1.6.1.4” on page 203, add the following to the existing list:

- Brocade 6505 24 ports
- Brocade VA-40FC 40 ports

Under the MIB object “connUnitPortIndex 1.3.6.1.3.94.1.10.1.2” on page 209, add the following to the existing list:

- Brocade 6505 24 ports
- Brocade VA-40FC 40 ports

Under the MIB object “connUnitPortPhysicalNumber 1.3.6.1.3.94.1.10.1.18” on page 214, add the following to the existing list:

- Brocade 6505 24 ports
- Brocade VA-40FC 40 ports

Chapter 11, FCIP MIB Objects

Add the following note to the MIB objects listed in [Table 2](#).

NOTE

This object is not supported.

TABLE 2 Not supported MIB objects

Object	OID	On page
fcipExtendedLinkTcpDroppedPackets	1.3.6.1.4.1.1588.4.1.1.3	240
fcipExtendedLinkTcpSmoothedRTT	1.3.6.1.4.1.1588.4.1.1.5	240
fcipExtendedLinkRtxRtxTO	1.3.6.1.4.1.1588.4.1.1.9	240
fcipExtendedLinkRtxDupAck	1.3.6.1.4.1.1588.4.1.1.10	240
fcipExtendedLinkDupAck	1.3.6.1.4.1.1588.4.1.1.11	240
xfcipExtendedLinkTcpDroppedPackets	1.3.6.1.4.1.1588.4.2.1.5	241

11 Documentation updates for Fabric OS v7.0.1

Fabric OS Troubleshooting and Diagnostics Guide

In this chapter

The updates in this chapter are for the *Fabric OS Troubleshooting and Diagnostics Guide*, publication number 53-1002150-02, published June 2011.

- [Documentation updates for Fabric OS v7.0.0 and later](#) 33
- [Documentation updates for Fabric OS v7.0.1 and later](#) 34

Documentation updates for Fabric OS v7.0.0 and later

Appendix A, Switch Type and Blade ID

In Table 22 on page 108, change the switch type of the B-Series switch model 5410 from 69 to 70. Also add entries for the Brocade 5470, 6510, and DCX 8510 Backbone family platforms. The revised information is as follows:

TABLE 22 switchType to B-series model converter

switchType	B-Series switch model	ASIC	Base switch speed
70	5410	GoldenEye2	8 Gb 12-port embedded switch
73	5470	GoldenEye2	8 Gb 20-port embedded switch
109	6510	Condor3	16 Gb 48-port switch
120	DCX 8510-8	Condor3	16 Gb 384-port core fabric backbone
121	DCX 8510-4	Condor3	16 Gb 192-port core fabric backbone

In Table 23 on page 108, add the following entries:

TABLE 23 B-series blade model descriptions

Blade ID	B-Series blade model	ASIC	Description
37	FC8-16	Condor2	8 Gb 16-FC ports blade
96	FC16-48	Condor3	16 Gb 48-FC ports blade
97	FC16-32	Condor3	16 Gb 32-FC ports blade

Documentation updates for Fabric OS v7.0.1 and later

Chapter 10, Diagnostic Features

In the section “Diagnostic Port” on page 92, in the fourth paragraph, change the second sentence from this:

D_Port configuration fails if the port is configured in R_RDY mode, encryption mode, or compression mode.

To this:

D_Port configuration fails if the port is configured in encryption mode or compression mode.

In the procedure for configuring a D_Port diagnostics session on page 93, add the following note after step 2:

If you are using D_Ports on active DWDM links, use the **dwdm** option on the **portcfgdport --enable** command.

In the section “D_Port limitations” on page 95, after the sentence “D-Port functionality is not supported with:” remove the following bullet item:

- R_RDY mode

Appendix A, Switch Type and Blade ID

In Table 22 on page 108, add the following entry:

TABLE 22 switchType to B-series model converter

switchType	B-Series switch model	ASIC	Base switch speed
118	6505	Condor3	16 Gb 24-port switch

In Table 23 on page 108, add the following entries:

TABLE 23 B-series blade model descriptions

Blade ID	B-Series blade model	ASIC	Description
125	FC8-32E	Condor3	8 Gb 32-FC ports blade
126	FC8-48E	Condor3	8 Gb 48-FC ports blade

Fabric Watch Administrator's Guide

In this chapter

The updates in this chapter are for the *Fabric Watch Administrator's Guide*, publication number 53-1002153-03, published April 2011.

- [Documentation updates for Fabric Watch v7.0.0 and later](#) 35

Documentation updates for Fabric Watch v7.0.0 and later

Chapter 1. Fabric Watch

In the existing “Fabric Watch licensing” section, the following paragraph is incorrect:

Fabric Watch is an optionally-licensed feature of Fabric OS. Each switch within a fabric needs its own license, and that license is valid only for a particular version of the feature. If you want a newer version of the feature, you must purchase a new license.

This paragraph should read as follows:

Fabric Watch is a optionally-licensed feature of Fabric OS. Once you purchase a Fabric Watch license for a platform, the license remains valid for the life of that platform and across firmware versions that are supported on that platform.

The following is *new* licensing information and should be added as a subheading to “Fabric Watch licensing:”

Universal temporary license support

The Fabric Watch license is available as a Universal Temporary or a regular temporary license, meaning the same license key can be installed on any switch running Fabric OS version 6.3 or later. Universal temporary license keys can only be installed once on a switch, but can be applied to as many switches as required. Temporary use duration (the length of time the feature will be enabled on a switch) is provided with the license keys.

Chapter 8. System Monitoring

The following information does not currently exist in the *Fabric Watch Administrator's Guide*, and will be added at the next major release of Fabric OS:

The default Fabric Watch policy for the Brocade DCX 8510-8 with total power consumption of more than 2000w does not properly reflect the switch status on the power supply. Fabric Watch users must manually update their default configuration for the minimum number of power supplies to three if they have installed more than 256 ports in an 8510-8 chassis.

Chapter 9. Fabric Watch configuration using Web Tools

The following, incorrect paragraph was removed from the note in the “Configuring Threshold Traits” section on page 91:

To set a Custom Defined percentage, use a corresponding value between 0.0 and 10.0. For example, to set a range of values of 53 percent through 77 percent, your Low Boundary value is 5.3 and the High Boundary value is 7.7.

Web Tools Administrator's Guide

In this chapter

The updates in this chapter are for the *Web Tools Administrator's Guide*, publication number 53-1002152-01, published April 2011.

- [Documentation updates for Fabric OS v7.0.0](#) 37
- [Documentation updates for Fabric OS v7.0.1](#) 37

Documentation updates for Fabric OS v7.0.0

Chapter 9, Administering Zoning

Under the heading of “Setting the default zoning mode” on page 119, add the following note:

NOTE

You should not change the default zone mode from No Access to All Access if there is no effective zone configuration and more than 120 devices are connected to the fabric.

Documentation updates for Fabric OS v7.0.1

About This Document

Under the heading “Supported hardware and software” on page xxiii, add the following to the existing list of supported hardware.

- Brocade 6505
- Brocade FC8-32E port blade
- Brocade FC8-48E port blade

Chapter 1, Introducing Web Tools

Under the heading “System requirements” on page 5, add “Firefox 3.6” under Browser column to the Windows Server 2008 R2 Standard (64-bit), Windows Server 2008 Standard, and Windows Vista Business platforms; replace “Internet Explorer 7.0” with “Firefox 3.6” for the Red Hat Enterprise Server 5 Advanced Platform and SUSE Linux Enterprise Server 10.

Chapter 2, Using the Web Tools Interface

Under the heading “Working with Web Tools: recommendations” on page 29, replace the following bullet.

Original:

- A maximum of five simultaneous HTTP sessions to any one switch is recommended. An HTTP session is considered a Fabric Manager or Web Tools connection to the switch.

Replacement:

- A maximum of five simultaneous HTTP sessions to any one switch is recommended. An HTTP session is considered a Brocade Network Advisor or Web Tools connection to the switch.

Chapter 6, Managing Ports

Under the heading “Configuring FC ports” on page 79, add the following note.

NOTE

With Fabric OS v7.0.1, Web Tools supports interoperability between a Fabric OS fabric and a Brocade Network OS fabric through an FC router. You can select this interoperability mode in the FC Port Configuration Wizard.

Under the heading “Allowed port types” on page 81, update the following information to include Brocade FC8-32E, Brocade FC8-48E, and Brocade 6505:

L_Ports are not supported on the Brocade FC16-32, Brocade FC16-48, or Brocade 6510.

Under the heading “Port activation” on page 86, add the following row to Table 9.

TABLE 9 Ports enabled with POD licenses and DPOD feature

Switch name	Enabled by default	Enabled with Ports on Demand licenses	Enabled with the Dynamic Ports on Demand feature
Brocade 6505	0-11	12-23	Not supported

Chapter 11, Using the FC-FC Routing Service

Under the heading “Supported switches for Fibre Channel Routing” on page 146, update the following information to include FC8-32E and FC8-48E:

Brocade DCX 8510-4 and DCX 8510-8, when configured with FC16-32 or FC16-48 blades.

Under the heading “FC-FC routing management” on page 147, add the following note:

NOTE

From Fabric OS v7.0.1, Integrated Routing (IR) license is not required to configure a port as EX_Port with Brocade Native mode and Brocade NOS mode.

Under the heading “Opening the FC Routing module” on page 147, add the following bullet:

- Brocade DCX 8510-4 and DCX 8510-8, when configured with FC8-32E or FC8-48E blades.

Under the heading “Configuring an EX_Port” on page 149, add the following note.

NOTE

With Fabric OS v7.0.1, Web Tools supports interoperability between a Fabric OS fabric and a Brocade Network OS fabric through an FC router. You can select this interoperability mode in the FC Port Configuration Wizard.

Chapter 14, Administering Extended Fabrics

Under the heading “Configuring a port for long distance” on page 167, add Brocade VA-40FC, Brocade 8000, and Brocade 6505 to step 4.

Chapter 15, Routing Traffic

Under the heading “Viewing fabric shortest path first routing” on page 170, add Brocade 6505 to step 3.

Under the heading “Lossless dynamic load sharing” on page 171, add Brocade 6505 to the list of platforms.

Under the heading “Configuring the link cost for a port” on page 173, add Brocade 7800, Brocade 6510, Brocade 6505, and Brocade VA-40FC to step 3.

Chapter 17, Administering FICON CUP Fabrics

Under the heading “FICON CUP fabrics overview” on page 215, replace the following text:

Original:

A Brocade switch or director that supports CUP can be controlled by one or more host-based management programs or director consoles, such as Brocade Web Tools or Brocade Fabric Manager. (Refer to the Fabric Manager Administrator’s Guide for information about Fabric Manager.) The director allows control to be shared between host-based management programs and director consoles.

Replacement:

A Brocade switch or director that supports CUP can be controlled by one or more host-based management programs or director consoles, such as Brocade Web Tools or Brocade Network Advisor. (Refer to the *Brocade Network Advisor SAN User Manual* for more information about the Brocade Network Advisor.) The director allows control to be shared between host-based management programs and director consoles.

14 Documentation updates for Fabric OS v7.0.1

Brocade 6510 Hardware Reference Manual

In this chapter

The updates in this chapter are for various hardware manuals.

- [Chapter 2, Brocade 6510 Installation and Configuration](#). 41
- [Appendix A, Brocade 6510 Specifications](#). 41

Chapter 2, Brocade 6510 Installation and Configuration

Under the heading “Local time synchronization” on page 11, replace the paragraph that says:

If the active NTP server configured is IPv6, then distributing the same in the fabric will not be possible to switches earlier than v5.3.0 because IPv6 is supported for Fabric OS version 5.3.0 and later. The default value LOCL will be distributed to pre-5.3.0 switches.

with the following paragraph:

If the active NTP server configured is IPv6, then distributing the same information in the fabric will not be possible to switches earlier than v5.3.0 because IPv6 is supported for Fabric OS version 5.3.0 and later. The default value LOCL will be distributed to pre-5.3.0 switches.

Under the heading “Setting the date” on page 11, replace the text for step 2 with the following:

2. Enter the **date** command, using the following syntax (the double quotation marks are required):

```
date "mmddHHMMyy"
```

Appendix A, Brocade 6510 Specifications

Under the heading “General specifications” on page 33, replace the information in Table 9 in the Description column for the Switching capacity information with the following information.

Specification	Description
Switching capacity	An aggregate switching capacity of 420 million frames per second (for Class 2, Class 3, and Class F frames for the 48 port chassis)

Brocade DCX 8510-8 Backbone Hardware Reference Manual

In this chapter

The updates in this chapter are for various hardware manuals.

- [Chapter 5, Removal and Replacement Procedures](#) 43

Chapter 5, Removal and Replacement Procedures

All of the following occurs under the heading “WWN card removal and replacement.”

Under the subheading “Determining the status of a WWN card” on page 87, replace the information in Table 12 in the Sample error message column for the WWN unit is being faulted row with the following information:

Type of message	Sample error message
WWN unit is being faulted.	<pre>0x24c (fabos): Switch: switchname, Critical EM-WWN_UNKNOWN, 1, Unknown WWN #2 is being faulted or 2010/09/16-13:44:21, [EM-1003], 40, SLOT 7 FFDC CHASSIS, CRITICAL, Brocade_DCX, WWN 2 has unknown hardware identifier: FRU faulted</pre>

Before the subheading “Removing the WWN card and WWN bezel (logo plate)” on page 88, add the following section:

Preparing for the WWN card replacement

If the WWN card requires replacement, complete the following steps.

ATTENTION

Follow ESD precautions (see “ESD Precautions” in your chassis manual).

1. Open a Telnet session to the chassis and log in to the active CP as admin. The default password is “password”.
2. Verify that you are logged into the active CP. Run the **haShow** command to determine the active CP.
3. Run the **supportsave** command on the active CP to capture all settings.

4. Contact Brocade Technical Support for a replacement WWN card. Technical Support will require the `supportsave` data collected in the previous step so that a replacement can be programmed prior to shipping to your location.

DO NOT execute the `frureplace` command. The command will no longer be functional beginning with the release of Fabric OS 7.0.0c, but users with earlier versions of the Fabric OS should also NOT run the command.

Under the subheading “Removing the WWN card and WWN bezel (logo plate)” on page 88, replace the steps with the following:

When the replacement WWN card has been received, complete the following steps to remove the bezel and faulted WWN card.

ATTENTION

Follow ESD precautions (see “ESD Precautions” in your chassis manual).

1. Open a Telnet session to the chassis and log in to the active CP as admin. The default password is “password”.
2. Verify that you are logged into the active CP. Run the `haShow` command to determine the active CP.
3. Run the `supportsave` command on the active CP to capture all settings. If any problems occur during the replacement, the information will be important for solving the problem.
4. Remove the screws from the WWN bezel. Pull the bezel away from chassis and set it aside. The WWN cards are visible.
5. Use a Phillips screwdriver to unscrew the two screws that secure the WWN card to the chassis. Hold the card by the edges and remove it.
6. Disconnect the WWN cable by depressing the cable connector latch and pulling the connector from the WWN module.
7. Set the WWN card on a static-free surface, such as a grounding pad.

Under the subheading “Replacing the WWN bezel (logo plate) and WWN card” on page 90, delete steps 3 and 4.

Brocade DCX 8510-4 Hardware Reference Manual

In this chapter

The updates in this chapter are for various hardware manuals.

- [Chapter 5, Removal and Replacement Procedures](#) 45

Chapter 5, Removal and Replacement Procedures

All of the following occurs under the heading “WWN card removal and replacement.”

Under the subheading “Determining the status of a WWN card” on page 81, replace the information in Table 11 in the Sample error message column for the WWN unit is being faulted row with the following information:

Type of message	Sample error message
WWN unit is being faulted.	<pre>0x24c (fabos): Switch: switchname, Critical EM-WWN_UNKNOWN, 1, Unknown WWN #2 is being faulted or 2010/09/16-13:44:21, [EM-1003], 40, SLOT 7 FFDC CHASSIS, CRITICAL, Brocade_DCX, WWN 2 has unknown hardware identifier: FRU faulted</pre>

Before the subheading “Removing the WWN card and WWN bezel (logo plate)” on page 82, add the following section:

Preparing for the WWN card replacement

If the WWN card requires replacement, complete the following steps.

ATTENTION

Follow ESD precautions (see “ESD Precautions” in your chassis manual).

1. Open a Telnet session to the chassis and log in to the active CP as admin. The default password is “password”.
2. Verify that you are logged into the active CP. Run the **haShow** command to determine the active CP.
3. Run the **supportsave** command on the active CP to capture all settings.

4. Contact Brocade Technical Support for a replacement WWN card. Technical Support will require the supportsave data collected in the previous step so that a replacement can be programmed prior to shipping to your location.

DO NOT execute the **frureplace** command. The command will no longer be functional beginning with the release of Fabric OS 7.0.0c, but users with earlier versions of the Fabric OS should also NOT run the command.

Under the subheading “Removing the WWN card and WWN bezel (logo plate)” on page 82, replace the steps with the following:

When the replacement WWN card has been received, complete the following steps to remove the bezel and faulted WWN card.

ATTENTION

Follow ESD precautions (see “ESD Precautions” in your chassis manual).

1. Open a Telnet session to the chassis and log in to the active CP as admin. The default password is “password”.
2. Verify that you are logged into the active CP. Run the **haShow** command to determine the active CP.
3. Run the supportsave command on the active CP to capture all settings. If any problems occur during the replacement, the information will be important for solving the problem.
4. Remove the screws from the WWN bezel. Pull the bezel away from chassis and set it aside. The WWN cards are visible.
5. Use a Phillips screwdriver to unscrew the two screws that secure the WWN card to the chassis. Hold the card by the edges and remove it.
6. Disconnect the WWN cable by depressing the cable connector latch and pulling the connector from the WWN module.
7. Set the WWN card on a static-free surface, such as a grounding pad.

Under the subheading “Replacing the WWN bezel (logo plate) and WWN card” on page 83, delete steps 3 and 4.

Brocade DCX Backbone Hardware Reference Manual

In this chapter

The updates in this chapter are for various hardware manuals.

- [Chapter 5, Removal and Replacement Procedures](#) 47

Chapter 5, Removal and Replacement Procedures

All of the following occurs under the heading “Removal and replacement of the WWN card.”

Under the subheading “Determining the status of a WWN card” on page 73, replace the information in Table 12 in the Sample error message column for the WWN unit is being faulted row with the following information:

Type of message	Sample error message
WWN unit is being faulted.	<pre><timestamp>, [EM-1034], <sequence-number>,, ERROR, <system-name>, WWN # set to faulty, rc=<return code> or <timestamp>, [EM-1003], 40, SLOT 7 FFDC CHASSIS, CRITICAL, Brocade_DCX, WWN 2 has unknown hardware identifier: FRU faulted</pre>

Before the subheading “Removing the WWN card and WWN bezel (logo plate)” on page 74, add the following section:

Preparing for the WWN card replacement

If the WWN card requires replacement, complete the following steps.

ATTENTION

Follow ESD precautions (see “ESD Precautions” in your chassis manual).

1. Open a Telnet session to the chassis and log in to the active CP as admin. The default password is “password”.
2. Verify that you are logged into the active CP. Run the **haShow** command to determine the active CP.
3. Run the **supportsave** command on the active CP to capture all settings.

4. Contact Brocade Technical Support for a replacement WWN card. Technical Support will require the `supportsave` data collected in the previous step so that a replacement can be programmed prior to shipping to your location.

DO NOT execute the `frureplace` command. The command will no longer be functional beginning with the release of Fabric OS 7.0.0c, but users with earlier versions of the Fabric OS should also NOT run the command.

Under the subheading “Removing the WWN card and WWN bezel (logo plate)” on page 82, replace the steps with the following:

When the replacement WWN card has been received, complete the following steps to remove the bezel and faulted WWN card.

ATTENTION

Follow ESD precautions (see “ESD Precautions” in your chassis manual).

1. Open a Telnet session to the chassis and log in to the active CP as admin. The default password is “password”.
2. Verify that you are logged into the active CP. Run the `haShow` command to determine the active CP.
3. Run the `supportsave` command on the active CP to capture all settings. If any problems occur during the replacement, the information will be important for solving the problem.
4. Remove the screws from the WWN bezel. Pull the bezel away from chassis and set it aside. The WWN cards are visible.
5. Use a Phillips screwdriver to unscrew the two screws that secure the WWN card to the chassis. Hold the card by the edges and remove it.
6. Disconnect the WWN cable by depressing the cable connector latch and pulling the connector from the WWN module.
7. Set the WWN card on a static-free surface, such as a grounding pad.

Under the subheading “Replacing the WWN bezel (logo plate) and WWN card” on page 83, delete step 4.

In this chapter

The updates in this chapter are for various hardware manuals.

- [Chapter 5, Removal and Replacement Procedures](#) 49

Chapter 5, Removal and Replacement Procedures

All of the following occurs under the heading “Removal and replacement of the WWN card.”

Under the subheading “Determining the status of a WWN card” on page 68, replace the information in Table 11 in the Sample error message column for the WWN unit is being faulted row with the following information:

Type of message	Sample error message
WWN unit is being faulted.	<pre><timestamp>, [EM-1034], <sequence-number>,, ERROR, <system-name>, WWN # set to faulty, rc=<return code> or <timestamp>, [EM-1003], 40, SLOT 7 FFDC CHASSIS, CRITICAL, Brocade_DCX, WWN 2 has unknown hardware identifier: FRU faulted</pre>

Before the subheading “Removing the WWN card and WWN bezel (logo plate)” on page 69, add the following section:

Preparing for the WWN card replacement

If the WWN card requires replacement, complete the following steps.

ATTENTION

Follow ESD precautions (see “ESD Precautions” in your chassis manual).

1. Open a Telnet session to the chassis and log in to the active CP as admin. The default password is “password”.
2. Verify that you are logged into the active CP. Run the **haShow** command to determine the active CP.
3. Run the **supportsave** command on the active CP to capture all settings.

4. Contact Brocade Technical Support for a replacement WWN card. Technical Support will require the `supportsave` data collected in the previous step so that a replacement can be programmed prior to shipping to your location.

DO NOT execute the `frureplace` command. The command will no longer be functional beginning with the release of Fabric OS 7.0.0c, but users with earlier versions of the Fabric OS should also NOT run the command.

Under the subheading “Removing the WWN card and WWN bezel (logo plate)” on page 69, replace the steps with the following:

When the replacement WWN card has been received, complete the following steps to remove the bezel and faulted WWN card.

ATTENTION

Follow ESD precautions (see “ESD Precautions” in your chassis manual).

1. Open a Telnet session to the chassis and log in to the active CP as admin. The default password is “password”.
2. Verify that you are logged into the active CP. Run the `haShow` command to determine the active CP.
3. Run the `supportsave` command on the active CP to capture all settings. If any problems occur during the replacement, the information will be important for solving the problem.
4. Remove the screws from the WWN bezel. Pull the bezel away from chassis and set it aside. The WWN cards are visible.
5. Use a Phillips screwdriver to unscrew the two screws that secure the WWN card to the chassis. Hold the card by the edges and remove it.
6. Disconnect the WWN cable by depressing the cable connector latch and pulling the connector from the WWN module.
7. Set the WWN card on a static-free surface, such as a grounding pad.

Under the subheading “Replacing the WWN bezel (logo plate) and WWN card” on page 70, delete steps 3 and 4.