

DCX FCIP Impl-2
Rev. 2.0 - 06 January 2016



8510 FCIP Implementation

Vodafone



Author Daniel Francois
Project No. 0005141

BROCADE



ADX, Brocade, Brocade Assurance, Brocade One, the B-wing symbol, DCX, Fabric OS, ICX, MLX, MyBrocade, SAN Health, VCS, and VDX are registered trademarks, and AnyIO, HyperEdge, NET Health, OpenScript, and The Effortless Network are trademarks 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 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

North America and Latin America Headquarters Corporate Headquarters

Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
Email: info@brocade.com

Beijing Brocade Communications Systems
Rm2718, South Kerry Center office Building
1 Guanghua Road
Chaoyang District
Beijing 100020
China
Tel: +86 10 6588 8888
Fax: +86 10 6588 9999
E-mail: china-info@brocade.com

European, Middle East and Africa 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 56 40
Fax: +41 22 799 56 41
E-mail: emea-info@brocade.com

Confidentiality Notice

This document contains confidential and proprietary information of **Brocade Communications Systems Inc.**, and **Vodafone** and may not be shared with any other party. Do not copy or disclose without the prior written permission of **Brocade** and **Vodafone**.

Document Revision History

Version	Date	Author	Description
0.1	15/12/2014	Daniel Francois	First draft version
1.0	18/12/2014	Daniel Francois	Final version
2.0	05/01/2016	Daniel Francois	Updated with added hardware

Contents

1 CONTACT INFORMATION	1
1.1 BROCADE CONTACT INFORMATION	1
1.2 VODAFONE CONTACT INFORMATION.....	1
1.3 VODAFONE LOCATIONS AND DATACENTRES.....	1
1.4 EMC CONTACT INFORMATION	1
2 REQUIRED INFORMATION	2
2.1 OVERVIEW OF TASKS.....	2
2.2 BILL OF MATERIAL	2
2.3 NAMING	3
2.4 TOPOLOGY	3
2.5 DOMAIN IDs AND FABRIC IDs	3
2.5.1 Fabric ID Assignment.....	3
2.5.2 Domain ID per Device.....	4
2.5.3 DCX Configuration.....	4
2.6 MANAGEMENT INTERFACE.....	5
2.6.1 IP Addresses	5
2.6.2 Applicable IP Filter	6
2.6.3 General Management Parameters	7
2.7 FCIP TUNNEL DEFINITION.....	7
3 DCX IMPLEMENTATION CHECKLIST	9
3.1 SITE CHECK AND SWITCH PREPARATION	9
3.2 PREPARE REMOTE SWITCH.....	9
3.3 DCX CONFIGURATION	10
3.4 FCIP TUNNEL CONFIGURATION.....	14
3.4.1 FCIP Tunnel Configuration.....	14
3.5 BNA IMPLEMENTATION	16
3.5.1 Check Switch Discovery.....	16
3.5.2 Check Registration of Syslogd Destination	17
3.5.3 Activate the custom MAPS policy.....	17
APPENDIX A: BROCADE DOCUMENTATION	19
APPENDIX B: PORTS MANAGEMENT FOR LOGICAL SWITCH.....	20
B.1: Assign Ports to a Logical Switch	20
B.2: Configure Ports for Devices.....	20
B.3: Configure Ports for ISL.....	20
APPENDIX C: FCIP OPTIONS	21
C.1: Tunnel Options	21
C.2: Circuit Options.....	24
APPENDIX D: FX8-24 OVERVIEW.....	27
D.1: Hardware overview	27
D.2: FX8-24 Blade License Options.....	27
D.3: VE_Ports and FCIP Tunnels	28
D.4: FCIP Trunking Capability.....	28
D.5: FCIP Circuits	28

APPENDIX E: VIRTUAL FABRIC AND FX8-24 **30**

E.1:	Virtual Fabric considerations	30
E.2:	Port sharing.....	30
E.3:	Limitations.....	30

APPENDIX F: FABRIC WATCH..... **31**

List of Tables

Table 1 – Contact Information: Brocade	1
Table 2 – Contact Information: Vodafone	1
Table 3 – Vodafone Locations	1
Table 4 – Contact Information: EMC	1
Table 5 – High Level Overview of Implementation Tasks for DCX.....	2
Table 6 – Bill of Material.....	2
Table 7 – Switch and Chassis Name.....	3
Table 8 – Fabric IDs: Defined Ranges.....	3
Table 9 – Domain ID per Device.....	4
Table 10 – DCX Configuration	4
Table 11 – Default IP Addresses for DCX.....	5
Table 12 – Defined IP Addresses for DCX.....	6
Table 13 – IP Filter Definition	6
Table 14 – IP Services	7
Table 15 – Gigabit Ethernet Interface Configuration	7
Table 16 – FCIP Tunnel Definition.....	8
Table 17 – Site Check and Switch Preparation	9
Table 18 – Prepare Remote Switch.....	10
Table 19 – A: Chassis Settings	10
Table 20 – B: Logical Switch Definitions.....	12
Table 21 – D: Switch Configuration.....	12
Table 22 – F: Switch Status Verification	13
Table 23 – G: Save Configuration.....	13
Table 24 – H: Merge Fabric	14
Table 25 – L: FX8-24 Link Configuration	14
Table 26 – FCIP Tunnel Options	21
Table 27 – FCIP Tunnel Options for FICON	22
Table 28 – FCIP Circuit Options.....	24
Table 29 – FX8-24 Licensed Features	27
Table 30 - VE Port Numbering	28

List of Figures

Figure 1 – Logical view one of two fabrics	3
Figure 2 – Discover Fabrics: Main Screen	16
Figure 3 – Add Fabric Discovery: Details	16

1 Contact Information

1.1 Brocade Contact Information

Table 1 – Contact Information: Brocade

Contact/Role	Office	Cell	Email
Aylin Koca	Istanbul	+ 90 532 591 54 03	akoca@brocade.com
Ufuk Baris	Istanbul	+90 212 340 76 61	ubaris@Brocade.com
Daniel Francois	Amsterdam	+ 31 6 8321 6926	dfrancoi@brocade.com

1.2 Vodafone Contact Information

Table 2 – Contact Information: Vodafone

Contact/Role	Office	Cell	Email
Mustafa Cakmakci	Istanbul	+908505420000	Mustafa.Cakmakci@vodafone.com
Umit Ozdemir	Istanbul	+908505420000	Umit.Ozdemir@vodafone.com

1.3 Vodafone Locations and Datacentres

Table 3 – Vodafone Locations

Location	Address
Vodafone Plaza	Büyükdere Caddesi No: 251

1.4 EMC Contact Information

Table 4 – Contact Information: EMC

Contact/Role	Office	Cell	Email
Mehmet Ozdemir	Istanbul		mehmet.ozdemir@emc.com
Cenk Bayraktar	Istanbul		Cenk.Bayraktar@emc.com

2 Required Information

2.1 Overview of Tasks

Table 5 – High Level Overview of Implementation Tasks for DCX

Step	Task
1.	Confirm engagement requirements
2.	Prepare installation area.
3.	Record equipment ID numbers.
4.	Connect power and grounding.
5.	Connect communications cables.
6.	Verify connectivity
7.	Power up equipment.
8.	Verify/load system software/firmware.
9.	Configure equipment. Persistently disable VE_Ports. If required, configure VEX_Ports. For the 7800 switch, set the media type for GbE ports 0 and 1. For the FX8-24 blade, set the GbE port operating mode. Assign IP addresses to the GbE ports. Create one or more IP routes using the portCfg iproute command. Test the IP connection using the portCmd -ping command. Create FCIP tunnels and FCIP circuits, and enable or disable features. Persistently enable the VE_Ports.
10.	Integrating new equipment in existing fabrics
11.	Complete installation tests.
12.	Provide End User with as-built documentation.

2.2 Bill of Material

Table 6 – Bill of Material

Short Name	Description	DCX Slots	Comment	Status
8510-8	16Gbps Director Condor3 Chassis	N/A		
CP16	Control processor blade for DCX	6,7		
CR16	Core Switching Blade w/ 2 ICL Ports	5,8		
FC16-48	48 Ports 16Gbps Condor3 Blade			
FX8-24	8Gbps FCIP Extension Blade	4		

2.3 Naming

Table 7 – Switch and Chassis Name

Device	Chassis Name	SwitchName
8510-8	IZMFSW15_C	IZMFSW15
8510-8	IZMFSW16_C	IZMFSW16
8510-8	IZMFSW17_C	IZMFSW17
8510-8	IZMFSW18_C	IZMFSW18
8510-8	ESNSW05_C	ESNSW05
8510-8	ESNSW06_C	ESNSW06
8510-8	ESNSW07_C	ESNSW07
8510-8	ESNSW08_C	ESNSW08
8510-8	ESNSW09_C	ESNSW09
8510-8	ESNSW10_C	ESNSW10

2.4 Topology

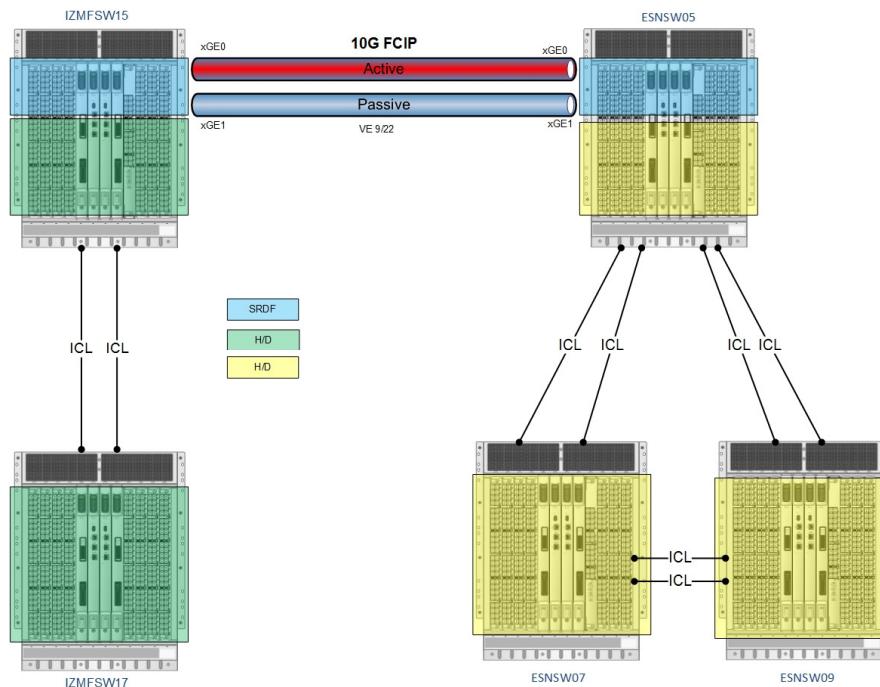


Figure 1 – Logical view one of two fabrics

2.5 Domain IDs and Fabric IDs

2.5.1 Fabric ID Assignment

Table 8 – Fabric IDs: Defined Ranges

Purpose	Range	Range length
Domain ID	171-186	16
Virtual Fabric FID	100-128	29

2.5.2 Domain ID per Device

Table 9 – Domain ID per Device

Device	Assigned Domain ID	Comment
IZMFSW15	171	
IZMFSW16	172	
IZMFSW17	172	
IZMFSW18	174	
ESNSW05	181	
ESNSW06	182	
ESNSW07	183	
ESNSW08	184	
ESNSW09	185	
ESNSW10	186	

2.5.3 DCX Configuration

Table 10 – DCX Configuration

DCX					
Switch Name	Logical Switches				
	VF ID	Switch Name	Domain ID	Address Mode	XISL
IZMFSW15_C	128	IZMFSW15	171	0	No
	100	IZMFSW15_SRDF	171	0	No

8510 - 8					
Switch Name	Logical Switches				
	VF ID	Switch Name	Domain ID	Address Mode	XISL
IZMFSW16_C	128	IZMFSW16	172	0	No
	100	IZMFSW16_SRDF	172	0	No

8510 - 8					
Switch Name	Logical Switches				
	VF ID	Switch Name	Domain ID	Address Mode	XISL
IZMFSW17_C	128	IZMFSW17	173	0	No

8510 - 8					
Switch Name	Logical Switches				
	VF ID	Switch Name	Domain ID	Address Mode	XISL
IZMFSW18_C	128	IZMFSW17	174	0	No

8510 - 8					
----------	--	--	--	--	--

8510 - 8						
Switch Name	Logical Switches					
	VF ID	Switch Name	Domain ID	Address Mode	XISL	
ESNSW05_C	128	ESNSW05	181	0	No	
	100	ESNSW05_SRDF	181	0	No	

8510 - 8						
Switch Name	Logical Switches					
	VF ID	Switch Name	Domain ID	Address Mode	XISL	
ESNSW06_C	128	ESNSW06	182	0	No	
	100	ESNSW06_SRDF	182	0	No	

8510 - 8						
Switch Name	Logical Switches					
	VF ID	Switch Name	Domain ID	Address Mode	XISL	
ESNSW07_C	128	ESNSW07	183	0	No	

DCX8510 - 8						
Switch Name	Logical Switches					
	VF ID	Switch Name	Domain ID	Address Mode	XISL	
ESNSW08_C	128	ESNSW08	184	0	No	

8510 - 8						
Switch Name	Logical Switches					
	VF ID	Switch Name	Domain ID	Address Mode	XISL	
ESNSW09_C	128	ESNSW09	185	0	No	

DCX8510 - 8						
Switch Name	Logical Switches					
	VF ID	Switch Name	Domain ID	Address Mode	XISL	
ESNSW10_C	128	ESNSW10	186	0	No	

2.6 Management Interface

2.6.1 IP Addresses

Table 11 – Default IP Addresses for DCX

Purpose	#	Default IP Address	Default NetMask
CP 0	1	10.77.77.75	255.255.255.0
CP 1	1	10.77.77.74	255.255.255.0
chassis / default LS	1	10.77.77.77	255.255.255.0
logical switch	max 7	n/a	n/a

Table 12 – Defined IP Addresses for DCX

Switch	Purpose	IP Address	Default NetMask	Default Gateway
IZMFSW15	CP 0	172.31.45.41	255.255.255.0	172.31.45.1
	CP 1	172.31.45.42	255.255.255.0	172.31.45.1
	chassis	172.31.45.43	255.255.255.0	
IZMFSW16	CP 0	172.31.45.44	255.255.255.0	172.31.45.1
	CP 1	172.31.45.45	255.255.255.0	172.31.45.1
	chassis	172.31.45.46	255.255.255.0	
IZMFSW17	CP 0	172.31.45.47	255.255.255.0	172.31.45.1
	CP 1	172.31.45.48	255.255.255.0	172.31.45.1
	chassis	172.31.45.49	255.255.255.0	
IZMFSW18	CP 0	172.31.45.50	255.255.255.0	172.31.45.1
	CP 1	172.31.45.51	255.255.255.0	172.31.45.1
	chassis	172.31.45.52	255.255.255.0	
ESNSW05	CP 0	10.86.6.153	255.255.255.192	10.86.6.129
	CP 1	10.86.6.154	255.255.255.192	10.86.6.129
	chassis	10.86.6.155	255.255.255.192	
ESNSW06	CP 0	10.86.6.156	255.255.255.192	10.86.6.129
	CP1	10.86.6.157	255.255.255.192	10.86.6.129
	chassis	10.86.6.158	255.255.255.192	
ESNSW07	CP 0	10.86.7.130	255.255.255.128	10.86.7.129
	CP1	10.86.7.131	255.255.255.128	10.86.7.129
	chassis	10.86.7.132	255.255.255.128	
ESNSW08	CP 0	10.86.7.138	255.255.255.128	10.86.7.129
	CP1	10.86.7.139	255.255.255.128	10.86.7.129
	chassis	10.86.7.140	255.255.255.128	
ESNSW09	CP 0	10.86.7.133	255.255.255.128	10.86.7.129
	CP1	10.86.7.134	255.255.255.128	10.86.7.129
	chassis	10.86.7.135	255.255.255.128	
ESNSW10	CP 0	10.86.7.141	255.255.255.128	10.86.7.129
	CP1	10.86.7.142	255.255.255.128	10.86.7.129
	chassis	10.86.7.143	255.255.255.128	

2.6.2 Applicable IP Filter**Table 13 – IP Filter Definition**

Rule	Source IP	Protocol	Dest Port	Action	Remark
1	any	tcp	22	permit	Permit SSH - default
2	any	tcp	23	deny	Deny Telnet - modified
3	any	tcp	897	permit	Permit API - default
4	any	tcp	898	permit	Permit API - default
5	any	tcp	111	permit	Permit RPC - default
6	any	tcp	80	deny	Permit HTTP - default
7	any	tcp	443	permit	Permit HTTPS - default
8	any	udp	161	permit	Permit SNMP - default
9	any	udp	111	permit	Permit PRC - default
10	any	udp	123	permit	Permit NTP - default
11	any	tcp	600 – 1023	permit	Permit DCFM - default
12	any	udp	600 – 1023	permit	Permit DCFM - default

2.6.3 General Management Parameters

Table 14 – IP Services

Parameter	Value	Comment
FTP Server		
Syslog Destination		
SNMP – Trap recipient		
SNMP – System Location		
SNMP – System Description		
SNMP – System Contact		
NTP – Time Server	10.74.0.135 / 10.74.0.136	
NTP – Time Zone	Europe / Istanbul	
DNS – Domain Name		
DNS – Server 1		
DNS – Server 2		

2.7 FCIP Tunnel Definition

Table 15 – Gigabit Ethernet Interface Configuration

IZMFSW15_SRDF					
GE Int. #	Type	Ip Address	Subnet Mask	Gateway	MTU
xge0	Op	10.183.10.82	255.255.255.252	10.83.10.80	1500
xge1	Op	10.183.10.86	255.255.255.252	10.183.10.85	1500

ESNSW05_SRDF					
GE Int. #	Type	Ip Address	Subnet Mask	Gateway	MTU
xge0	Op	10.183.12.10	255.255.255.252	10.183.12.9	1500
xge1	Op	10.183.12.12	255.255.255.252	10.183.12.11	1500

IZMFSW16_SRDF					
GE Int. #	Type	Ip Address	Subnet Mask	Gateway	MTU
xge0	Op	10.183.10.90	255.255.255.252	10.183.10.89	1500
xge1	Op	10.183.10.94	255.255.255.252	10.183.10.93	1500

ESNSW06_SRDF					
GE Int. #	Type	Ip Address	Subnet Mask	Gateway	MTU
xge0	Op	10.183.12.18	255.255.255.252	10.183.12.17	1500
xge1	Op	10.183.12.22	255.255.255.252	10.183.12.21	1500

Table 16 – FCIP Tunnel Definition

IZMFSW15_SRDF - ESNSW05_SRDF							
Ve	Switch	IP Address	Remote Switch	Remote IP Address	Bandwidth -B -b	Compression level	Metric
9/22.0	IZMFSW15_SRDF	10.183.10.82	ESNSW05_SRDF	10.183.12.10	10G - 6G	C 1	0
9/22.1	IZMFSW15_SRDF	10.183.10.86	ESNSW05_SRDF	10.183.12.12	10G - 6G	C 1	1

IZMFSW16_SRDF - ESNSW06_SRDF							
Ve	Switch	IP Address	Remote Switch	Remote IP Address	Bandwidth -B -b	Compression level	Metric
9/22.0	IZMFSW16_SRDF	10.183.10.90	ESNSW06_SRDF	10.183.12.18	10G - 6G	C 1	0
9/22.1	IZMFSW16_SRDF	10.183.10.94	ESNSW06_SRDF	10.183.12.22	10G - 6G	C 1	1

3 DCX Implementation Checklist

3.1 Site Check and Switch Preparation

Table 17 – Site Check and Switch Preparation

#	Task Description	ToDo	Status
S.1	Physical inspection	Inspect rack, power, cooling and cabling	
S.2	Power up DCX	Check all components and status leds	
S.3	Physical connect the management network	Connect management network to both CP blades	
S.4	Connect serial connection to active CP Terminal Settings: ⇒ 9600 Bits per second ⇒ 8 Data bits ⇒ No parity ⇒ 1 Stop bit ⇒ No Flow control	Connect to serial port of DCX using the connection cable provided by Brocade.	
S.5	Login credentials Standard username and password: ⇒ Userid: admin ⇒ Password: password	Login as admin Change all 4 password accordingly	
S.6	Interface setting	➤ ifmodeset eth0	
S.7	Connect serial connection to StandBy CP	Connect to serial port of DCX using the connection cable provided by Brocade.	
S.8	Login credentials	Login as admin	
S.9	Interface setting	Login as admin ➤ ifmodeset eth0	
S.10	Connect serial connection to active CP	Connect to serial port of DCX using the connection cable provided by Brocade.	
S.11	Login credentials	Login as admin	
S.12	Set IP addresses ⇒ Refer to Table 12 for defined IP Addresses	➤ ipaddrset -cp 0 ➤ ipaddrset -cp 1 ➤ ipaddrset -chassis	
S.13	Run system verification ⇒ OEM responsibility to test the hardware	Login as root ➤ systemverification	

3.2 Prepare Remote switch

When the new DCX is connected to an existing fabric all the defined ISL ports on the remote switch should be persistently disabled in order to reduce the risk of a fabric merge during the configuration of the new device.

The ISL ports on the remote switch will be enabled after the configuration of the new switch is completed and validated.

Table 18 – Prepare Remote Switch

#	Task Description	ToDo	Status
R.1	Disable all ISL ports	➢ portcfgpersistentdisable [<slot>/]<port>	
R.2	Open E_Port functionality	➢ portcfgeport [<slot>/]<port> 1	
R.7	Enable ICL Ports ⇒ Slot 5 ports 384-415 ⇒ Slot 6 ports 416-447	➢ portcfgpersistentenable [<slot>/]<port>	
R.8	Cable ICL following admin guide and release notes		

3.3 DCX Configuration

Configuration steps:

- DCX Configuration
 - A: Chassis Settings
 - B: Logical Switch Definitions
 - D: Switch Configuration
 - F: Switch Status Verification
 - G: Save Configuration
 - H: Merge Fabric
- FCIP Configuration
 - L: FX8-24 Link Configuration

Table 19 – A: Chassis Settings

#	Task Description	ToDo	Status
A			
A.1	Verify Firmware	➢ version ➢ firmwareshow	
A.2	Upgarde Fabric OS		
A.2a	Upgrade FOS using USB key	➢ usbstorage -e ➢ firmwaredownload -U <firmware folder name>	
A.2b	Upgrade FOS from FTP server	➢ firmwaredownload	
A.3	Verify firmware upgrade	➢ firmwarestatusshow ➢ version ➢ firmwareshow	
A.4	Make choice to enable or disable Virtual Fabrics functionality ⇒ Switch reboots after changing this setting (cold reboot and disruptive)		
A.4a	➔ enable Virtual Fabrics	➢ fosconfig --enable vf	
		➢	
A.5	Reset switch configuration	➢ configdefault -all	
A.6	Set chassis name	➢ chassisname <name of chassis>	
A.7	Validate all licenses	➢ licenseshow	

#	Task Description	ToDo	Status
A.8	7. Install required licensed	<ul style="list-style-type: none"> ➢ licenseidshow ⇒ Follow the procedure defined by the OEM to generate license keys ➢ licenseadd <license key> 	
	⇒	<ul style="list-style-type: none"> ➢ 	
A.10	Define NTP server ⇒ check Table 14 for defined parameters	<ul style="list-style-type: none"> ➢ tsclockserver <ip address> 	
A.11	Set time zone ⇒ check Table 14 for defined parameters	<ul style="list-style-type: none"> ➢ tstimezone <GEO/City> 	
A.12	Define syslog destination ⇒ check Table 14 for defined parameters	<ul style="list-style-type: none"> ➢ syslogdipadd <ip address> 	
A.13	Enable audit logging	<ul style="list-style-type: none"> ➢ auditcfg --enable 	
A.14	Enable audit class	<ul style="list-style-type: none"> ➢ auditcfg --class 1,2,3,4,5,7,8,9 ➢ 	
A.16	Define SNMP v3 parameters	<ul style="list-style-type: none"> ➢ snmpconfig --set snmpv3 ⇒ 	
A.18	Set telnet timeout	<ul style="list-style-type: none"> ➢ timeout <minutes> ➢ 	
A.19	Define IP Filter for IP v4 ⇒ check Table 13 for the IP Filter settings to apply	<ul style="list-style-type: none"> ➢ ipfilter --clone vodafone_custom -from default_ipv4 ➢ ipfilter --addrule Vodafone_custom -rule 2 -sip any -dp 23 -proto tcp -act deny ➢ ipfilter --delrule vodafone_custom -rule 3 ➢ ipfilter --save vodafone_custom ➢ ipfilter --activate vodafone_custom 	
A.22	Define personalized accounts	<ul style="list-style-type: none"> ➢ userconfig --add bna_admin -r admin -l 1-128 -h 128 -c admin -d "Admin user for BNA" 	BrOcade12
A.22A	Create an account for SNMP	<ul style="list-style-type: none"> ➢ userconfig --add snmpadmin1 -r admin -l 1-128 -h 128 -c admin -d "user for snmp" 	Brocade123
A.23	Check ICL ports are enabled. ICL ports: ⇒ Slot 5 ports 384-415 ⇒ Slot 6 ports 416-447	<ul style="list-style-type: none"> ➢ switchshow 	
A.23a	➔ enable ICL	<ul style="list-style-type: none"> ➢ portenable <slot>/<port> ➢ portcfgpersistentenable <slot>/<port> 	
A.24	Enable MAPS	<ul style="list-style-type: none"> ➢ mapsconfig -enablenmaps -policy dfilt_moderate_policy 	
A.25	Clone default MAPS policy into a custom policy	<ul style="list-style-type: none"> ➢ mapsconfig --clone dfilt_moderate_policy -name vodafone_moderate_policy 	
A.26	Enable the Vodafone custom policy	Via BNA customize and export/import the vodafone_moderate_policy.xml	

Table 20 – B: Logical Switch Definitions

#	Task Description	ToDo	Status
B	Create Base or Logical Switches. ⇒ Repeat for each logical switch ⇒ If no Logical Switches are deployed proceed to step C. ⇒ check Table 10 for defined Logical Switches		
B.1	Specify Logical Switch to Create: Setup logical switch. ⇒ XISL → Base LS ⇒ FCR → Base LS ⇒ Other → LS		
		➤	
B.1b	➔ create Logical Switch	➤ lscfg --create <FID>	100
B.2	Login to new Logical switch	➤ setcontext <FID>	100
B.3	Define port addressing mode and XISL usage ⇒ choose addressing mode ⇒ enable or disable XISL usage	➤ configure	
B.6	Assign ports to Logical of base switch	➤ lscfg --config 100 -slot <slot#> -port <port#>	

Table 21 – D: Switch Configuration

#	Task Description	ToDo	Status
D	Switch Configuration ⇒ applies to all switch types ⇒ repeat for each defined Logical Switch ⇒ check Table 10 for defined Logical Switches		
D.1	Connect to Logical Switch ⇒ only applies if Virtual Fabrics are deployed	Login as admin ➤ setcontext <FID>	
D.2	Purge existing zoning configuration	➤ cfgdisable ➤ cfgclear ➤ defzone --noaccess ➤ cfgsave	
D.3		➤	
D.4	Disable switch	➤ switchdisable	
D.5	Define switch name	➤ switchname <name switch>	
D.6	Configure Fabric Parameters ⇒ set domain ID ⇒ fix Insistent Domain ID ⇒ validate any other values	➤ configure Configure... Fabric parameters (yes, y, no, n): [no] y Domain: (1..239) [1] <DOMAIN ID> Insistent Domain ID Mode (yes,y,no,n):[no] <y>	
D.7	Setting fabric principal ⇒ only switches qualified as fabric principal	➤ farbicprincipal --enable -p <priority> (-f)	
D.8	Define Routing policies ⇒ Discuss the routing policy with the customer and check requirements.		
D.8c	➔ DPS on ➔ IOD set ➔ Lossless DLS	➤ aptpolicy 3 ➤ iodreset ➤ dlsset --enable -lossless	
D.8x..	

#	Task Description	ToDo	Status
D.10	Enable Trunking ⇒ Trunking license is required	➢ licenseshow ➢ portcfgtrunkport [<slot>/]<port> 1	
D.11	Persistentdisable all ports ⇒	➢ portcfgpersistentdisable <slot/port>	
D.12	Open E_Port functionality for ISL Ports	➢ portcfgeport [<slot>/]<port> 1	
D.17	Configure F ports If applicable: ⇒ block L_Port ⇒ block E_Port ⇒ set port speed	➢ portcfgport [<slot>/]<port> 1 ➢ portcfgport [<slot>/]<port> 0 ➢ portcfgspeed [<slot>/]<port> <speed> ➢ portcfgshow	
D.18	Enable the switch	➢ switchenable	
D.19	Bottleneck monitoring will be replaced by FPI in FOSv7.3x and higher	➢ bottleneckmon -disable ➢	
D.20	Define switch status policy	➢ switchstatuspolicyset ➢ switchstatuspolicyshow	

Table 22 – F: Switch Status Verification

#	Task Description	ToDo	Status
F	Verify Switch status		
F.1	Verify domain	➢ switchshow	
F.2	Verify security policy	➢ secpolicyshow	
F.3	Verify port settings	➢ portcfgshow	
F.4	Verify DCX overall health	➢ switchstatusshow ➢ fanshow ➢ sensorshow ➢ tempshow ➢ chassisshow ➢ slotshow ➢ portshow ➢ errshow	
F.5	Verify HA status	➢ hashow	
F.6	Clear all errors	➢ errclear ➢ slotstatsclear ➢ statsclear	

Table 23 – G: Save Configuration

#	Task Description	ToDo	Status
G	Save Configuration		
G.1	Save configuration ⇒ use BNA (DCFM) as alternative	➢ configupload -all	
G.2	Save support info ⇒ use BNA (DCFM) as alternative	➢ supportsave	
G.3	Perform San Health capture	DCX Requires SAN Health 3.1.4 or Later http://www.brocade.com/support/sanhealthdownload.jsp	

Table 24 – H: Merge Fabric

#	Task Description	ToDo	Status
H	Enable Switch and join fabric		
H.1	Enable DCX	➢ switchenable	
H.2	Enable ports (E and F ports)	➢ portcfgpersistenable [<slot>/]<port>	
H.3	Check configuration	➢ switchshow ➢ fabricshow ➢ errshow ➢ porterrshow (clear all counters after 10 minutes)	
H.4	Clear all errors after approximately 10 minutes	➢ errclear ➢ slotstatsclear ➢ statsclear	

3.4 FCIP Tunnel Configuration

3.4.1 FCIP Tunnel Configuration

Table 25 – L: FX8-24 Link Configuration

#	Task Description	ToDo	Status
L			
L.1	Configure GbE port operating mode ⇒ 1G: enable GbE ports 0 through 9 → XGE0 and XGE1 are disabled ⇒ 10G: enables XGE0 and XGE1 → ports Ge0-Ge9 are disabled ⇒ dual: enables GbE ge0-ge9 and XGE0 → XGE1 is disabled	➢ bladecfggemode --set 10G -slot 9	10G
L.2	Setting VE port to persistent disabled state	➢ portcfgshow ➢ portcfgpersistentdisable [<slot>/]<port>	
L.3	Configure a GbE or XGE port IP address ⇒ Refer to Table 15 for assigned IP Addresses	➢ portcfg ipif [<slot>/]<port> create <ip address> <netmask> <MTU>	
L.4	Define IP Route ⇒ skip if remote interface resides in same network	➢ portcfg iproute [<slot>/]<port> create <network address destination> <netmask> <gateway>	
L.5	Validate IP connectivity ⇒ works only if the steps L.1 to L.4 have been processed on the remote FCIP device	➢ portcmd --ping ge0 -s <src_ip> -d <dst_ip> ➢ portcmd --traceroute ge0 -s <src_ip> -d <dst_ip>	
L.6	Configuring tunnel ⇒ ARL minimum and maximum rates are set per circuit. They must be the same on either end of a circuit, but individual circuits may have different rates. ⇒ See Table 26 for more options on tunnel configuration	➢ portcfg fciptunnel slot/port create <src_ip> -d <dst_ip> -b <min-comm-rate> -B <max-comm-rate> -c 1 -x 0	

#	Task Description	ToDo	Status
L.7	Enable VE port	<ul style="list-style-type: none"> ➢ portcfgshow ➢ portcfgpersistenable <slot/port> 	
L.8	Check tunnel settings	<ul style="list-style-type: none"> ➢ portshow fc iptunnel all -c 	
L.9	Define additional FCIP Tunnel options ⇒ Discuss additional FCIP Tunnel options shown in C.1:	<ul style="list-style-type: none"> ➢ portcfg fc iptunnel [<slot/>] <port> modify -<option> <operand> 	
L.10	Create additional circuits into existing tunnel to form a FCIP Tunnel ⇒ The VE_Ports used to create the tunnel are the same as specified on the FCIP tunnel in the basic sample configuration. The VE_Ports uniquely identify the tunnel, and the circuit is associated with this specific tunnel. ⇒ ARL minimum and maximum rates are set per circuit. They must be the same on either end of a circuit, but individual circuits may have different rates. ⇒ See Table 28 for more options on circuit configuration	<ul style="list-style-type: none"> ➢ portcfg fc ip circuit slot/port create <circuit#> <src_ip> <dst_ip> -b <min-comm-rate> -B <max -comm-rate> 	
L.11	Define additional FCIP Circuit options ⇒ Discuss additional FCIP Circuit options shown in C.2:	<ul style="list-style-type: none"> ➢ portcfg fc ip circuit [<slot/>] <port> modify -<option> <operand> 	

3.5 BNA Implementation

3.5.1 Check Switch Discovery

1. Check if the switch or logical switches show up in BNA

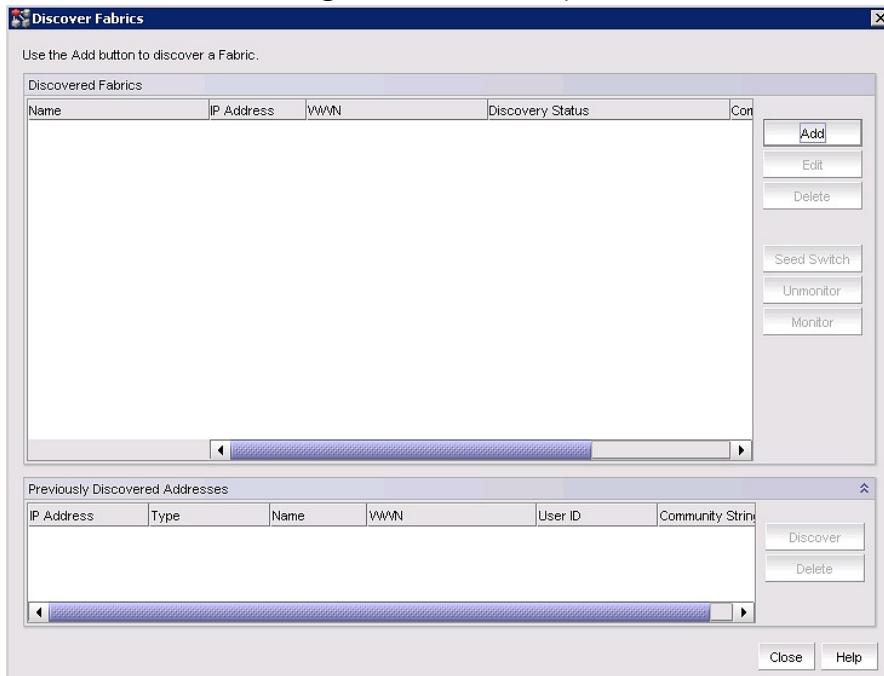


Figure 2 – Discover Fabrics: Main Screen

2. Discover the switch or logical switches in BNA

Note:

- ☞ This only has to be done if the switch or logical switches are not already discovered in BNA

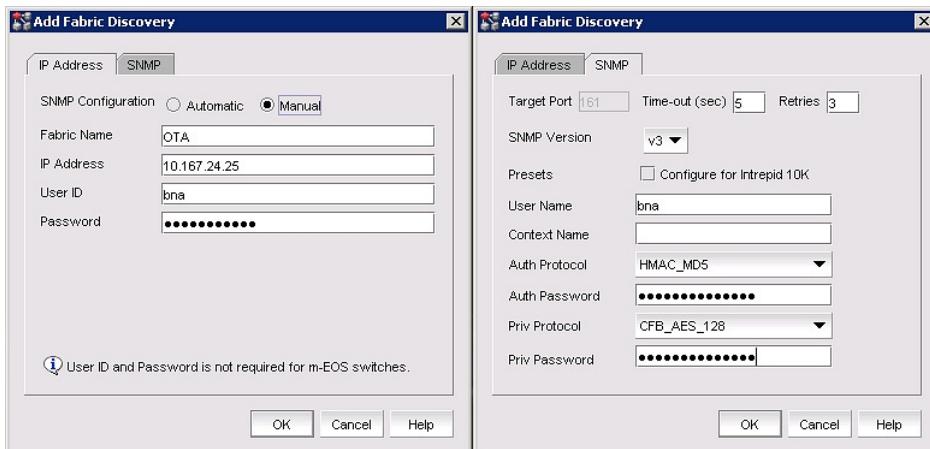


Figure 3 – Add Fabric Discovery: Details

ToDo:

- On the “Discover Fabrics” main screen click on “Add”
- Go to the “IP Address” tab
- Select “Manual” SNMP configuration

- Enter the IP Address details and credentials
- Go to the “SNMP” tap
- Enter the SNMP details and credentials

3.5.2 Check Registration of Syslogd Destination

3. Check registration of syslogd destination

```
syslogdipshow
syslog.1 10.165.132.13
```

ToDo:

- Check for the IP Address of the BNA Server: 10.165.132.13

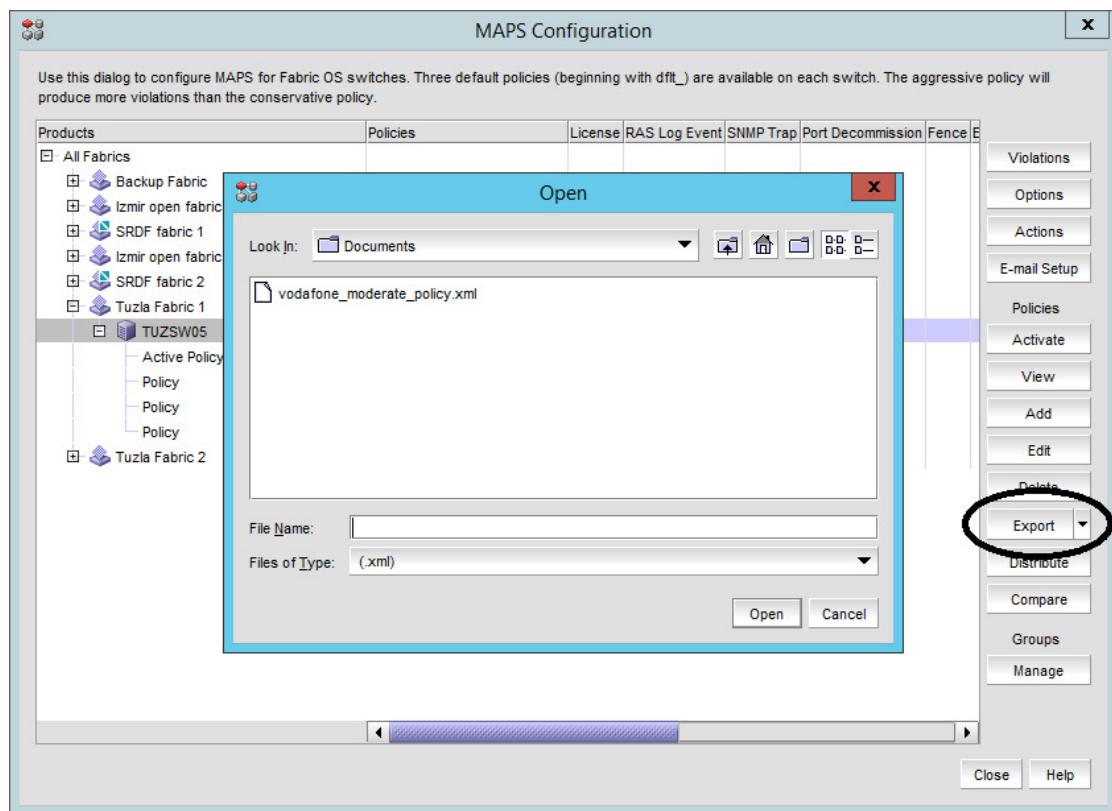
4. Define syslogd destination

Note:

- ☞ This only has to be done if the BNA server was not properly registered as syslogd destination

```
syslogdipadd 10.165.132.13
```

3.5.3 Activate the custom MAPS policy



ToDo:

- Click on the import button and select the custom policy Vodafone_moderate_policy.xml.
- Custom policies can also be Distributed to all or selected fabrics.



EMC²

BROCADE

8510 FCIP Implementation

Appendix A: Brocade Documentation

Communications documentation can be downloaded from the customer login web site:

http://www.brocade.com/forms/jsp/sic/SIC_Reg.jsp

Appendix B: Ports Management for Logical Switch

B.1: Assign Ports to a Logical Switch

While the environment growth, additional ports must be added to the different logical switches.

Remark

☞ Check for the latest version of the excel workbook.

If no ports are available a new port blade can be added to the switch.

1. The defined ports are added using the FOS command:

```
lscfg --config <FID> -port <port> -f
```

2. Disable all User Ports

```
portcfgpersistentdisable [<slot>/]<port>
```

3. Disable e-Port Capability on all User Ports

```
portcfgeport [<slot>/]<port> 0
```

B.2: Configure Ports for Devices

Applies to all devices such as HBA, Tape drives, Storage controllers ...

1. Enable the ports

```
portcfgpersistentenable [<slot>/]<port>
```

B.3: Configure Ports for ISL

1. Enable the ports

```
portcfgpersistentenable [<slot>/]<port>
```

2. Fix Port Speed on ISL Ports

```
portcfgspeed [<slot>/]<port>
```

3. Configure the E ports capability for ISLs

```
portcfgeport [<slot>/]<port> 1
```

Appendix C: FCIP Options

C.1: Tunnel Options

In this section you will find all tunnel options that can be configured for different scenarios. Discuss with End User and/or OEM/partner which options must be enabled and what the arguments should be. Document the options and arguments.

Table 26 – FCIP Tunnel Options

Option	Arguments	Disruptive	Description
Compression	Short option: -c <operand> Long option: --compression <operand> Operands: ⇒ 0 – Disable compression ⇒ 1 – Enables Standard compression ⇒ 2 – Enables Moderate compression ⇒ 3 – Enables Aggressive compression ⇒ 4 – Enables Auto compression mode	Yes	Enables compression on an FCIP tunnel. Compression is set by the portCfg fcipTunnel create or modify command, and applies to traffic over all circuits in the tunnel. Compression cannot be set or modified by the portCfg fcipCircuit create or modify command.
FCIP Fastwrite	Short Option: -f <operand> Long Option: --fast-write <operand> Operands: ⇒ None required for create ⇒ 0 – disables FCIP Fastwrite ⇒ 1 – enables FCIP Fastwrite	Yes	Disables or enables FCIP Fastwrite. A FCIP Fastwrite is initially disabled, and must be enabled to take effect.
OSTP	Short Option: -t <operand> Long Option: --tape-pipelining <operand> Operands: ⇒ None required for create ⇒ 0 – disable OSTP ⇒ 1 – enable OSTP Read/Write ⇒ 2 – enable OSTP Write	Yes	Disables or enables tape OSTP. OSTP is initially disabled. Both FCIP Fastwrite and OSTP must be enabled if you want to implement OSTP, as described in “Open Systems Tape Pipelining”
QoS Priority Percentages	Short option: ⇒ -q -high <operand> ⇒ -q -medium <operand> ⇒ -q -low <operand> Long option: ⇒ --qos-high <operand> ⇒ --qos-medium <operand> ⇒ --qos-low <operand> Operands: ⇒ Percentage values from 1-100	Yes	Sets Quality of Service (QoS) priority percentages to different values from default values of 50% for QoS high, 30% for QoS medium, and 20% for QoS low. Priorities are enforced only when there is congestion on the network. If there is no congestion, all traffic is handled at the same priority
Remote FC WWN	Short Option: -n <operand> Long Option: --remote-wwn <operand> Operands: ⇒ remote-WWN	Yes	This is a fabric security feature that allows you to only allow the FCIP tunnel to come up when the correct remote WWN is entered. If the WWN of the remote side does not match the value entered here, the FCIP tunnel will not initiate.
Enable IPSec	Short Option: -i <operand> Long Option: --ipsec <operand> Operands: ⇒ None required for create ⇒ 0 – disable IPSec ⇒ 1 – enable IPSec	Yes	Disables or enables IPsec on a FCIP tunnel.
Legacy IPSec connection	Short Option: -l <operand> Long Option: --legacy <operand> Operands: ⇒ None required for create ⇒ 0 – disable IPSec Legacy connection ⇒ 1 – enable IPSec Legacy connection	Yes	Disables or enables legacy IPsec mode. This mode uses the IPsec connection process compatible with Fabric OS versions prior to v7.0.0.

Option	Arguments	Disruptive	Description
IKE V2 authentication Key for IPSec	Short Option: -K Long Option: -key Operands for modify and create): ⇒ Pre-shared key	Yes	The pre-shared key used during IKE authentication.

Table 27 – FCIP Tunnel Options for FICON

Option	Arguments	Disruptive	Description
FICON emulation	Short Option: -F <operand> Long Option: -ficon <operand> Operands: ⇒ None required for create ⇒ 0 – disable IPSec Legacy connection ⇒ 1 – enable IPSec Legacy connection	Yes	Disables or enables FICON mode.
FICON XRC emulation	--ficon-xrc <operand> Operands: ⇒ 0 – disable FICON XRC emulation ⇒ 1 – enable FICON XRC emulation		FICON XRC Emulation allows XRC (IBM eXtendedRemote Copy, also known as IBM z/OS Global Mirroring) to operate effectively at extended distances.
FICON Tape Write Pipelining	--ficon-tape-write <operand> Operands: ⇒ 0 – disable FICON Tape Write Pipelining ⇒ 1 – enable FICON Tape Write Pipelining		This feature improves the performance of certain applications when writing to tape over extended distances.
FICON Tape Read Pipelining	--ficon-tape-read <operand> Operands: ⇒ 0 – disable FICON Tape Read Pipelining ⇒ 1 – enable FICON Tape Read Pipelining		This feature improves performance for certain applications when reading from FICON tape over extended distances.
FICON TIN/TIR emulation	--ficon-tin-tir <operand> Operands: ⇒ 0 – disable FICON TIN/TIR emulation ⇒ 1 – enable FICON TIN/TIR emulation		This feature enhances recovery when a TIN/TIR exchange occurs as part of a channel recovery operation during tape emulation.
FICON Device Level Acknowledgement emulation	--ficon-dvcack <operand> Operands: ⇒ 0 – disable FICON Device Level Acknowledgement emulation ⇒ 1 – enable FICON Device Level Acknowledgement emulation		This feature is applicable to both FICON Disk and Tape configurations. The feature removes one network round trip for exchanges that end with a Device Level Acknowledgement frame from the device.
FICON read Tape Read Block ID emulation	--ficon-read-blk <operand> Operands: ⇒ 0 – disable FICON read Tape Read Block ID emulation ⇒ 1 – enable FICON read Tape Read Block ID emulation		This feature permits FICON write channel programs containing embedded read block ID commands (CCWs) with a byte count of exactly four bytes to be processed as emulated commands during write emulation processes.
tape read channel commands (CCWs)	--max-read-pipe <operand> Operands: ⇒ Value 1 - 100		Defines the maximum number of tape read channel commands (CCWs) that can enter the read pipeline for a single device whether all the CCWs are bundled in a single channel program or in multiple channel programs. The setting has significance only for host (channel) initiated operations at this side and will not affect tape write operations initiated by hosts (channels) attached at the opposite side. Too small of a value will result in poor performance. The value should be chosen based upon the typical tape channel program that requires optimum performance. The default value is 32

Option	Arguments	Disruptive	Description
tape write channel commands (CCWs)	--max-write-pipe <operand> Operands: ⇒ Value 1 - 100		Defines the maximum number of tape write channel commands (CCWs) that can enter the write pipeline for a single device whether all the CCWs are bundled in a single channel program or in multiple channel programs. The setting has significance only for host (channel) initiated operations at this side and will not affect tape write operations initiated by hosts (channels) attached at the opposite side. Too small of a value will result in poor performance. The value should be chosen based upon the typical tape channel program that requires optimum performance. The default value is 32
number of concurrent emulated tape read operations	--max-read-devs <operand> Operands: ⇒ Value 1 - 32		Defines the maximum number of concurrent emulated tape read operations. As concurrency increases, the value of emulation decreases. Excessive concurrency has the potential to oversubscribe packet data memory. The setting has significance only for host (channel) initiated operations at this side and will not affect tape read operations initiated by hosts (channels) attached at the opposite side. The default value is 16
number of concurrent emulated tape write operations	--max-write-devs value <operand> Operands: ⇒ Value 1 - 32		Defines the maximum number of concurrent emulated tape write operations. As concurrency increases, the value of emulation decreases. Excessive concurrency has the potential to oversubscribe packet data memory. The setting has significance only for host (channel) initiated operations at this side and will not affect tape write operations initiated by hosts (channels) attached. The default value is 16
time limit for pipelined write chains	--write-timer <operand> Operands: ⇒ Time value 100 - 1500		Defines a time limit for pipelined write chains. This value is specified in ms. If a pipelined write chain takes longer than this value to complete, the ending status for the next write chain will be withheld from the channel. This limits processing to what the network and device can support. Too small a value limits pipelining performance. Too large a value results in too much data being accepted for one device on a path. The default value is 300 ms

Option	Arguments	Disruptive	Description
maximum amount of data in a single CCW chain	--write-chain <operand> Operands: ⇒ Time value 1 – 5		Defines the maximum amount of data in MB that can be contained in a single CCW chain. If this value is exceeded, emulation is suspended. The default value is 3 MB
base value of an entry pool of 256 OXIDs	--oxid-base <operand> Operands: ⇒ Hex value 0x0000 - 0xF000		Defines the base value of an entry pool of 256 OXIDs supplied to emulation-generated exchanges. It should fall outside the range used by FICON channels and devices to avoid conflicts. The default value is 0x8000. ⇒ Note that the default value has changed, and you no longer need to change the default value for any configuration.
Debug flags	--ficon-debug <operand> Operands: ⇒ Valid flag value		Defines optional debug flags. The default value is 0xF7C80000. This parameter is primarily for use by technical support personnel.

C.2: Circuit Options

In this section you will find all circuit options that can be configured for different scenarios. Discuss with End User and/or OEM/partner which options must be enabled and what the arguments should be. Document the options and arguments.

Table 28 – FCIP Circuit Options

Option	Arguments	Disruptive	Description
Committed rate	Only the operand is required. Operands: ⇒ Traffic rate in kbps 10000 - 1000000	Yes	Specifies the committed traffic rate on the FCIP tunnel in Kbps. The valid range is 10000 Kbps to 1000000 Kbps. There is no default. Both sides of the circuit must have matching configurations. ⇒ Alternately use Adaptive Rate Limiting (ARL).
Adaptive Rate Limiting (ARL)	Short option: -b Long option: --min-comm-rate Operands: ⇒ Traffic rate in kbps 10000 - 1000000 Short option: -B Long option: --max-comm-rate Operands: ⇒ Traffic rate in kbps 10000 - 1000000	Yes	The minimum committed rate is a guaranteed minimum traffic rate for an FCIP circuit. ⇒ When added together, the minimum committed rates for all circuits cannot exceed the speed of the GbE port. The maximum committed rate is the rate that the tunnel will try to achieve, based on bandwidth availability and network performance. ⇒ When ARL is used, The link cost is equal to the sum of maximum traffic rates of all established, currently active lowest metric circuits in the tunnel.

Option	Arguments	Disruptive	Description
Selective Acknowledgement	Short option: -s Long option: -sack Operands for create: ⇒ No operands are required. FICON emulation is enabled when specified on create. Operands for modify: ⇒ 0 – disable SACK ⇒ 1 – enable SACK	Yes	Disables or enables selective acknowledgement. Selective acknowledgement allows a receiver to acknowledge multiple lost packets with a single ACK response. This results in better performance and faster recovery time. Selective acknowledgement is initially turned on. For some applications and in some situations, you may need to turn selective acknowledgement off. This option is used to toggle the option off and on.
Keep alive timeout	Short Option: -k Long Option: -keepalive-timeout Operands: ⇒ Timeout value in ms	Yes	The keep-alive timeout in seconds. The range of valid values is 8 through 720000 ms, and the default is 1000ms (10s).
Minimum retransmit time	Short Option: -m Long Option: -min-retrans-time Operands: ⇒ Retransmit time in ms	No	The minimum retransmit time, in milliseconds. The range of valid values is 20 through 5000 ms and the default is 100 ms.
failover/standby metric	Short Option: -x Long Option: -metric Operands: ⇒ 0 – assigns higher priority on circuit ⇒ 1 – assigns lower priority on circuit	Yes	Specifies the metric for the configured circuit. A lower metric assigns a higher priority to the circuit. As data is flowing through the FCIP tunnel, it automatically traverses the lowest metric cost circuits. For example, if a tunnel has four circuits, three of which are set to a metric of 0 and one is set to a metric of 1, all data will flow over the metric 0 circuits. If all of the metric 0 circuits go down, traffic will run over the metric 1 circuit. This parameter is meaningful only, if you configure more than one circuit.
VLAN Tagging	Short Option: -v Long Option: -vlan-tagging Operands: ⇒ Valid VLAN ID ⇒ Layer 2 COS (see next row)	Yes	Applies VLAN tagging to a circuit and sets a specific Layer 2 Class Of Service (COS).
Class of Service (COS)	--l2cos-f-class <n> --l2cos-high <n> --l2cos-medium <n> --l2cos-low <n> Operands: ⇒ L2COS value 0 - 7	Yes	Sets the Layer 2 Class Of Service (l2cos) options for VLAN tagging. Options are for F-Class traffic, and high, medium, and low priority traffic.
DSCP Tagging	DSCP tag options (use with VLAN tagging options and operand): - -dscp-f-class <n> - -dscp-high <n> - -dscp-medium <n> - -dscp-low <n>	Yes	Applies a DSCP tag to a circuit
Specify connection type	Short Option: -C Long Option: -connection-type Operands: ⇒ default ⇒ listener ⇒ initiator	Yes	Allows you to specify which side of the circuit is the listener or initiator. If this is not specified, the initiator and listener is automatically selected based on the lower and higher-order IP address. In NAT environments, this can cause problems as both sides of the circuit may have lower-order addresses. When setting initiator or listener options, a firmware download to a previous version will not be allowed until you set the default option.

Option	Arguments	Disruptive	Description
Maximum retransmits	Short Option: -r Long Option: --max-retransmits Operands: ⇒ number of retransmits 1 - 16	No	Sets the maximum number of retransmits for the FCIP circuit before the connection will be brought down. If operating on a lossy network, increasing this value may allow the FCIP circuit to remain active when it may otherwise fail.
Administrative status	Short Option: -a Long Option: --admin-status Operands: ⇒ 0 – disable circuit ⇒ 1 – enable circuit	Yes	Disables or enables the FCIP circuit.

Appendix D: FX8-24 Overview

D.1: Hardware overview

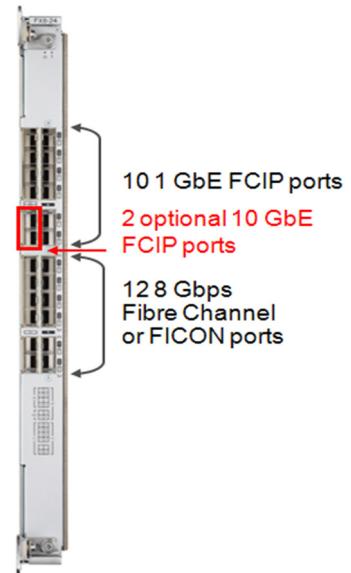
12x 8Gbps FC ports, numbered 0 through 11, are delivered on the FX8-24 blade. Each of these FC ports can operate at 1, 2, 4, or 8 Gbps.

In addition to the FC ports, 10x 1GbE ports, numbered 0 through 9, are implemented.

The ports xge0 and xge1 are 10GbE ports.

The FX8-24 blade provides a maximum of 20 Gbps of bandwidth for connections. There for the blade can operate in only one of three different modes:

- 1 Gbps mode
All ten GbE ports (0 through 9) are enabled
Both XGE ports are disabled
- 10 Gbps mode
All ten GbE ports (0 through 9) are disabled
Both XGE ports are enabled
- Dual mode
All ten GbE ports (0 through 9) are enabled
The 1st XGE (xge0) ports is enabled
The 2nd XGE (xge1) ports is enabled



The FX8-24 blade can be deployed in either a DCX or a DCX-4S chassis. Up to 4 FX8-24 blades are allowed per chassis.

D.2: FX8-24 Blade License Options

Some of the capabilities of the FX8-24 blade require the slot-based feature licenses shown in the table below. Use the FOS command “licenseshow” to display license keys and licenses currently installed.

Table 29 – FX8-24 Licensed Features

Feature	Purpose	License (licenseshow output)
10GbE support	Allows 10 Gbps operation on 10 GbE ports.	10 Gigabit FCIP/Fibre Channel (FTR_10G) license
Advanced FICON acceleration	Enables accelerated tape read/write, accelerated data mirroring over distance, and other features in FICON environments	Advanced FICON Acceleration (FTR_AFA) license
Integrated routing (IR)	Required to configure VEX_Ports to support Fibre Channel Routing (FCR).	Integrated Routing license
Advanced Extension License	Required for multiple-circuit tunnels, FCIP trunking, Adaptive Rate Limiting (ARL), and other FCIP features	Advanced Extension (FTR_AE) license

Note:

- ☞ This is a slot-based license for the FX8-24 and 7800.

D.3: VE_Ports and FCIP Tunnels**Table 30 - VE Port Numbering**

GE Port	VE Port Range
ge0	12
ge1	13
ge2	14
ge3	15
ge4	16
ge5	17
ge6	18
ge7	19
ge8	20
ge9	21
xge0	22-31
xge1	12-21

An FX8-24 blade can support 20 FCIP tunnels on 20 available VE_Ports. There are two VE_Port groups:

- Ports 12-21 associated to the ports ge0 to ge9 or xge1 used when FX8-24 is configured in 1 Gbps mode or 10 Gbps mode
- Ports 22-31 associated to port xge0 used when FX8-24 operates in 10Gbps mode or dual mode

Each FCIP tunnel will be associated with a specific VE_Port.

D.4: FCIP Trunking Capability

FCIP Trunking is a method for managing the use of WAN bandwidth and providing redundant paths over the WAN that can protect against transmission loss due to WAN failure. Trunking is enabled by creating logical circuits within an FCIP tunnel. A tunnel may have multiple circuits. Each circuit is a connection between a pair of IP addresses that are associated with source and destination endpoints of an FCIP tunnel.

FCIP trunking provides load leveling and failover capabilities through the use of multiple FCIP circuits.

D.5: FCIP Circuits

The following list describes FCIP circuit characteristics and usage.

- A circuit can have a maximum commit rate of 1 Gbps.
- Beginning with v6.4.0 the minimum committed rate allowed on a circuit is 10 Mbps. When upgrading to v6.4.0 from an earlier version, if there is a circuit configured with a minimum committed rate of less than 10 Mbps, the circuit will need to be updated to have a committed rate of no less than 10 Mbps.
- In a scenario where a FCIP tunnel has multiple circuits of different metrics, circuits with higher metrics are treated as standby circuits, and are not used until all lower metric circuits fail.

- An FCIP tunnel can have up to four circuits when using the 1GbE interfaces, They may be on the same 1GbE interface or spread out over up to four 1GbE interfaces.
- Committed bandwidth on both sides of the tunnels/circuits must be the same.
- The maximum bandwidth for a single circuit is 1 Gbps. To utilize the entire bandwidth of an XGE (10GbE) port, you must create ten 1 Gbps circuits within that interface.
- When load leveling across multiple circuits, the difference between the committed rate of the slowest circuit in the FCIP Trunk and the fastest circuit should be no greater than a factor of 4 (i.e. a 100 Mbps and a 400 Mbps circuit is OK, but a 10 Mbps and a 400 Mbps circuit is not OK). This ensures that the entire bandwidth of the FCIP Trunk can be utilized. If you configure circuits with the committed rates that different by more than a factor of 4, the entire bandwidth of the FCIP Trunk may not be fully utilized.
- A circuit defines source and destination IP addresses on either end of an FCIP tunnel.
- If the circuit source and destination IP addresses are not on the same subnet, a IP static route must be defined which designates the gateway IP address.
- For IPv4 connections, multiple 1GbE or 10GbE ports on a FX8-24 blade or a 7800 switch cannot be on same subnet. For IPv6 connections, each GbE (or 10GbE) port needs to be connected to an interface that has a unique link local address. In other words multiple GbE ports on a 7800 or FX8-24 cannot connect to next hops with the same link local address.
These restrictions will be removed in a later release.

Tunnel and circuit requirements for FX8-24 Extension Blades are as follows:

- Up to 8 IP addresses can be configured for each GbE port.
- A FCIP Tunnel can be build using up to 10 circuits. These circuit can be defined:
 - on the 1 GbE port supporting 4 circuits per port
 - on the 10 GbE port supporting 10 circuits per port
- A limit of 20 FCIP circuits can be configured per VE port group (12 -21 or 22 - 31) when using a 10G port. For the 20 circuits, 10 are configured on local ports and 10 on crossports
- For a FX8-24 blade with a VE_Port group on a 10GbE port, the sum of the maximum committed rates of that group's primary circuits cannot exceed 10 Gbps. This same limit applies to secondary circuits.

Appendix E: Virtual Fabric and FX8-24

E.1: Virtual Fabric considerations

The 1GbE ports, 10GbE ports, and VE_Ports on the FX8-24 blade can be part of any logical switch and can be moved between any two logical switches. In addition, ports do not need to be off-line when they are moved.

Because GbE ports and VE_Ports are independent of each other, both must be moved in independent steps. The configuration on VE_Ports and GbE ports must be deleted before moving those ports between logical switches.

This differs from the FR4-18i blade, where when GbE ports are moved, all the VE_Ports created on that GbE port are automatically moved, and configurations do not need to be deleted.

E.2: Port sharing

In Fabric OS v7.0 and later, VE_Ports in different logical switches can share a single GbE port (1GbE or 10GbE) on the default switch.

Note:

- ☞ In Fabric OS versions prior to FOS 7.0 (6.4 and older), in order to use a GbE port for an FCIP tunnel, that port needed to be in the same logical switch as the VE_Port for the tunnel.

With GbE port sharing, you can have the following configuration, as an example:

- Default switch has port GbE0
- Logical switch 1 has VE13, which has a circuit over GbE0
- Logical switch 2 has VE14, which also has a circuit over GbE0
- etc...

All of the committed-rate restrictions and bandwidth sharing of the GbE ports for ARL remain the same for shared ports in the logical switches. VE_Ports created from shared GbE ports initiate as regular VE ISLs in their respective logical switches.

E.3: Limitations

Following limitations apply for port sharing:

- Only GbE ports in the default switch can be shared by VE_Ports in different logical switches. A GbE port in a non-default switch can only be used by VE_Ports in that same logical switch.
- The GbE ports in other logical switches or ports on the base switch cannot be shared by ports in different logical switches.
- Tunnels created with a mix of dedicated ports (ports within the same logical switch) and shared ports (ports in the default switch) are not supported.

Appendix F: Fabric Watch

Class	Area	Recommended customized (for RASLOG events/Port Fencing)								
		ALL_PORTS			E-PORTS			F-Port (Host)		
		AG	MO	CO	AG	MO	CO	AG	MO	CO
Port Thresholds	C3TX_TO	0/2	3/5	5/10	0/2	3/5	5/10	2/4	3/10	10/20
	CRC	0/2	10/20	20/40	0/2	10/20	20/40	0/2	10/20	20/40
	ITW	15/25	20/40	40/80	15/25	20/40	40/80	15/25	20/40	40/80
	Link Reset	2/4	5/10	10/20	2/4	5/10	10/20	2/4	5/10	10/20
	State Change	0/4	5/10	10/20	0/4	5/10	10/20	0/4	5/10	10/20
	Signal Loss	0/2	3/7	5/10	0/2	3/7	5/10	0/2	3/7	5/10
	Protocol Err									

3.5.3.1 Fabric, Security, SFP, Environment

Class	Area	Fabric Watch		
		High	Low	Buffer
VE- Circuit	State Change	1		
	Utilization %	75		
	Packet Loss	0.05		
Fabric	Fabric		0	
	Segmentation			
Resource	Flash (%)	90		
	CPU	75		
	Memory	80		