Brocade Fabric OS 4.1.1a

Release Notes

August 15, 2003

TABLE OF CONTENTS

General Information 4
Overview 4
About This Release 4
Supported Switches 4
Technical Support 4
Documentation 5
Supporting Documentation 5
Standards Compliance 5
New Features and Enhancements 6
Information About Secure Fabric OS 7
Information About FICON® 7
Documentation Addendum 8
SilkWorm 3900 (2109-F32) Hardware Reference Manual 8
Brocade ISL Trunking User's Guide, v3.1.0/4.1.0 8
Brocade Fabric OS Procedures Guide v4.1 8
Brocade Fabric OS Reference Guide v4.1 8
Requirements and Compatibility 9
Important Notes 9
SilkWorm 2000 (2109-S08/S16) Series Scalability Support 9
Maximizing Fabric Availability during SW 3900 (2109-F32) Hot Code Activation 9
Microsoft Internet Explorer Issue 9
Interpreting Ambient and Internal Temperatures 10
Other Important Notes: 10
Defects Closed In Fabric OS 4.1.1a 13

General Information

Fabric OS 4.1.1a is a patch release that contains fixes to a small number of additional issues detected. Brocade software release policy is to carry forward all fixes in patches to subsequent maintenance and feature releases of Fabric OS. Aside from these changes, it is functionally identical to Fabric OS 4.1.1. These Release Notes will refer to "Fabric OS 4.1" when making statements that apply to Fabric OS 4.1.0 and 4.1.1x.

Overview

About This Release

Fabric OS 4.1 represents the first major feature revision to the Fabric OS v4.0 firmware. It should be considered an upgrade and replacement for Fabric OS 4.0.0, which shipped initially with the launch of the 2109 Model M12 in the first half of 2002, and for Fabric OS 4.0.2, which shipped initially in the second half of 2002, supporting the 2109 Model F32 and M12.

Fabric OS v4.1.1a includes the following changes:

- Fixes to defects as detailed in the Defects Closed In Fabric OS 4.1.1a section.
- Correction to Fabric OS v4.1.0 and v4.1.1 Release Notes. The Documentation Addendum section of this document lists the changes. This is not a code change but a documentation correction only.
    - Documentation correction for scalability support limit for fabrics containing Fabric OS v2.6.1. This limit changes from 500 devices to 728 devices.

Supported Switches

Like Fabric OS 4.1.0, Fabric OS 4.1.1 supports both the 2109 Model M12 and F32.

Technical Support

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To assist your support representative and to expedite your call, have the following three sets of information immediately available when you call:

1. General Information

- Technical Support contract number, if applicable
- switch model
- switch operating system version
- error messages received
- **supportshow** command output
- detailed description of the problem and specific questions
- description of any troubleshooting steps already performed and results

2. Switch Serial Number

The switch serial number is provided on the serial number label, as shown below.

Type 2109-M12	**Type 2109-F32**
S/N PPSSSSS	**S/N PPSSSSS**

The serial number label is located as follows:

- *2109 Model S16, S08 switches:* Bottom of chassis
- *2109 Model F16 and 3534 Model F08 switches: Front and b*ottom of chassis
- *2109 Model F32 switches: Front and b*ottom of chassis
- *2109 Model M12 switches:* Inside front of chassis, on wall to left of ports

3. Worldwide Name (WWN)

- *2109 Model M12 and F32 switches:* Provide the license ID. Use the **licenseidshow** command to display the license ID.
- *All other switches:* Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Documentation

Supporting Documentation

Fabric OS 4.1.1 uses the same documentation as Fabric OS 4.1.0.

In addition to these release notes, this release is supported by the following documentation:

2109 switch documentation:

• IBM TotalStorage SAN Switch 2109 Model M12 User's Guide (GC26-7468-02).

• IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide (GC26-7467-03).

• IBM TotalStorage SAN Switch 2109 Model F32 User's Guide (GC26-7517-01).

• IBM TotalStorage SAN Switch 2109 Model F32 Installation and Service Guide (GC26-7496-02).

Fabric OS v4.1 software documentation:

• Brocade Fabric OS Reference

• Brocade Fabric OS Procedures Guide

• Brocade Advanced Zoning User’s Guide

• Brocade Advanced Web Tools User’s Guide

• Brocade Advanced Performance Monitoring User’s Guide

• Brocade Distributed Fabrics User’s Guide

• Brocade Fabric Watch User’s Guide

• Brocade ISL Trunking User’s Guide

• Brocade Secure Fabric OS User’s Guide

• Brocade MIB Reference

• Brocade Diagnostic and System Error Message Reference

These documents are provided in PDF format on the documentation CD-ROM provided with the switch or you can download at: http://www.storage.ibm.com/ibmsan/products/2109/library.html

Standards Compliance

Brocade Fabric OS v4.1 is compliant with the following Fibre Channel Standards:

- FC-AL ANSI X3.272: 1996

- FC-AL-2 NCIT S 332: 1999
- FC-FLA NCIT S TR-20: 1998
- FC-GS-3 NCITS 348-2000 Rev 7.01
- FC-FG ANSI X3.289: 1996
- FC-PH ANSI X3.230: 1994
- FC-PH-2 ANSI X3.297: 1997
- FC-PH-3 ANSI X3.303: 1998
- FC-PLDA NCIT S TR-19: 1998
- FC-SW-2 Rev 5.3
- FC-VI Rev 1.61
- FC-MI, Rev 1.92
- FC-SB-2 Rev 2.1 (FICON Support)
- FC-BB Rev 4.7
- FC-FS Rev 1.7 (Still in draft)
- FC-BB-2 Rev 5.3 (Still in draft)
- IPFC RFC 2625
- FCP ANSI X3.269: 1996
- FCP-2 Rev 7

New Features and Enhancements

Brocade Fabric OS v4.1 will provide the following enhancements and new features relative to Fabric OS 4.0.2:

- Additional High Availability features:
    - Non-disruptive code activation on 2109 Model M12 and F32 switches
    - Non-disruptive failover between CPs (Control Processors) on the 2109 Model M12
    - Additional background health monitoring of the Standby CP on the 2109 Model M12
    - Managed hot swap procedure for the 2109 Model M12 WWN / status card
- Support for the optionally licensed Secure Fabric OS product. Secure Fabric OS includes the following features:
    - A new, centralized fabric management model, in which all fabric-wide management operations must originate from the Fabric Configuration Server, or “trusted switch”
    - Management Access Controls to secure and limit all means of switch and fabric management
    - Switch Connection Controls and Device Connection Controls, which strictly control what switches and devices may participate in the fabric.
    - Standards-based authentication (using digital certificates and PKI, or Public Key Infrastructure) of all switches in the fabric, to prevent unauthorized switches from joining the fabric.
    - A workstation-based utility, PKICERT, to acquire and install digital certificates for all switches in the fabric which do not already have them. The digital certificates are required to enable secure mode.
- Zoning enhancements:

    - New commands for searching the Zoning data base
    - Improved performance
    - More selective SCNs – they are now sent only to devices in zones where there has been a status change among the online members of those zones.

- WebTools enhancements:
    - Replacement of the Fabric View panel with a "switch explorer" tree – an approach which allows WebTools to handle larger fabrics more efficiently

- Disabling and enabling of ports and of entire switches may now be made persistent across reboots and power cycles.

- Fabric Time Service
    - Synchronizes time among switches in the fabric
    - Fabric time may be set from a CLI session or obtained from an external NTP server

- A new fabricPrincipal command allows the administrator to give a switch preference in negotiating to become principal switch in a fabric. This can be useful in optimizing the efficiency of fabric configurations and management operations.

- Fabric Watch enhancements:
    - Improved reporting of port and switch uptime statistics

- Ports may be configured to negotiate directly to R_RDY flow control mode, simplifying operations by allowing the connection of many WAN gateway products without requiring a Remote Switch license.

Information About Secure Fabric OS

Brocade's Secure Fabric OS® is a comprehensive security product that requires some planning and specific steps to set up and configure. For this purpose, the following document should be reviewed as a minimum of preparation prior to getting started:

- *Secure Fabric OS Quick Start Guide*

More detailed product information may be obtained from the *Secure Fabric OS Users Guide*.

Information About FICON®[1]

The Fabric OS version 4.1.0 and 4.1.1 releases contain code to allow FICON capable hosts and storage systems to connect to the 2109 Model M12 and transmit FICON data. However, Brocade's OEM partners have not yet begun the testing and qualification of Brocade's FICON support in their mainframe and storage environments. For this reason, the Fabric OS 4.1 code should NOT be used for FICON product qualification, end user FICON beta testing, or end user deployment in FICON environments. Brocade continues to test its support for FICON extensively and will provide a release supported for FICON deployments upon completion of FICON environment qualification testing by Brocade and its partners.

[1] FICON is a registered trademark of IBM Corporation in the U.S. and other countries.

Documentation Addendum

This section provides information on last minute additions to the documentation.

In Fabric OS v4.1.0 and v4.1.1 Release Notes, the 2109 Model S16/S08 Scalability Limit section specifies that fabrics containing Fabric OS v2.6.1 or later should not exceed 500 user (non-ISL) ports or devices. Brocade has increased to 728 devices as the maximum number of devices supported in fabrics that include 2109 Model S16/S08 series switches running Fabric OS v2.6.1 or later. This is only a change to the documentation. There is no change to the Fabric OS.

SilkWorm 3900 (2109-F32) Hardware Reference Manual
(publication number 53-0001595-02)

The following statement should be added to the Port Status LED information for when the port status is "offline" in Table 3-1 "Port Side LED Patterns During Normal Operation", on page 3-2.

"When a Port Status LED indicator light is off, another possible hardware status is offline."

Brocade ISL Trunking User's Guide, v3.1.0/4.1.0
(publication number 53-0000520-02)

Page 1-3 of the Brocade ISL Trunking User's Guide, v3.1.0/4.1.0 contains the following statement:

"... ISL Trunking does not support the "LE", "L1", or "L2" **portcfglongdistance** modes. For information about these modes and Extended Fabrics in general, refer to the *Distributed Fabrics User's Guide*."

This statement should be modified to say the following:

"...Trunking is supported for normal E_Ports (referred to as L0 in the **portcfglongdistance** command) with LWL media up to 5km at the full speed permitted by the link. With LWL media, the throughput begins to fall off beyond 5km, due to normal latency effects. ISL Trunking does not support the "LE", "L1", or "L2" **portcfglongdistance** modes. For information about these modes and Extended Fabrics in general, refer to the *Distributed Fabrics User's Guide*."

Brocade Fabric OS Procedures Guide v4.1
(publication number 53-0000501-02)

The following information should be to Step 7, of the procedure for "Upgrading the Firmware on the SilkWorm 12000" (2109-M12) in chapter 4.

"When the v4.1.0 firmware is unzipped, it creates a folder and a set of firmware files. Use the following directory and file name when downloading this firmware to the switch: /v4.1.0/release.plist.

For the User prompt enter a User ID that has an account on the FTP server."

Brocade Fabric OS Reference Guide v4.1
(publication number 53-0000519-02)

The following note should added to the **firmwaredownload** command:

"The User ID required for the firmwaredownload process must have an account on the FTP server."

Requirements and Compatibility

Brocade Fabric OS v4.1.0 and v4.1.1 can be installed and run on the 2109 Model M12 and F32.

The following table summarizes the versions of Brocade firmware and software that are supported in conjunction with these releases:

	2109-S08/S16 3534-1RU	**2109-F16 3534-F08**	**2109-F32**	**2109-M12**	**Fabric Manager**
General compatibility	2.6.0c or later	3.0.2c or later	4.0.2 or later	4.0.0c or later	3.0.2c or later
With Secure Fabric OS enabled	2.6.1 or later	3.1.0 or later	4.1.0 or later	4.1.0 or later	3.0.2c or later
Recommended adjacent to 2109-F32s running 4.1.0 or later	2.6.1 or later	3.1.0 or later	4.1.0 or later	4.1.0 or later	3.0.2c or later

Note: For the Fabric OS v2.x switches or Fabric OS v3.x switches, the Core Switch PID Format must be enabled (that is, set to 1) using the **configure** command before it can interconnect with the 2109 Model M12 and F32. For more information regarding the Core Switch PID Format, please refer to "Updating the Core PID Format" in the *Fabric OS Procedures Guide*.

Important Notes

2109 Model S16 and S08 Scalability Support

Exhaustive testing has demonstrated that 2109 Model S16 and S08 switches should not be deployed in fabrics that exceed 728 SAN devices.

Maximizing Fabric Availability during 2109-F32 Hot Code Activation

During code activation on a 2109-F32 running Fabric OS 4.1.0 or later, data keeps flowing between hosts and storage devices. However, fabric services are unavailable for a period of approximately 50-55 seconds. Possible disruption of the fabric can be minimized by ensuring that switches logically adjacent to the 2109-F32 (directly connected via an ISL) are running Fabric OS 2.6.1 or later, 3.1.0 or later, or 4.1.0 or later. More information is available in the Firmware Download section of the Fabric OS Procedures manual.

Microsoft Internet Explorer Issue

An issue has been identified with Microsoft Internet Explorer 5.0 and 5.5 running on Windows NT 4.0. The problem is as follows. Normally, when you launch a copy of the Switch Explorer applet, the left hand panel displays a tree of switches in your fabric. Clicking on a tree node will cause the right hand panels to refresh to the currently selected switch. However, under NT/4.0 and IE 5.0/5.5, the right hand panel will NOT update for the 2nd and subsequent instance of the Switch Explorer. Only the first instance works.

This issue has been identified and confirmed by Microsoft. For details, see the URL http://support.microsoft.com/default.aspx?scid=KB;en-us;242167&.

Workaround: There are 2 workarounds for this:
1. Always use a single instance of the SwitchExplorer on NT/4.0 and IE 5.0/5.5
2. Install IE 6.0 SP1

Alternatively, it is possible that you can obtain a workaround directly from Microsoft for this problem. Please contact Microsoft support and supply them the information in the defect as described in the URL http://support.microsoft.com/default.aspx?scid=KB;en-us;242167&.

Interpreting Ambient and Internal Temperatures

Brocade's SilkWorm fabric switches are instrumented with temperature sensors to monitor the operating characteristics of the products and their environment. The following table explains how to interpret the various temperature readings that may be reported via Fabric OS v4 and monitored via the Fabric Watch optional licensed firmware product. All temperatures are degrees C.

Sensor	Minimum	Maximum	Comments
2109 Model M12			
Blowers	0	40	Sensor on each blower measures inlet (ambient) air temperature
Port Blades	0	74	Each port blade has its own temperature sensor. Warning at 75° C. blade shutdown at 80° C.
CP Blades	0	74	Each CP blade has its own temperature sensor. Warning at 75° C.; CP will be faulted at 80° C.
2109 Model F32			
Switch	0	69	Switch sends warning at internal temperature of 67° C. Switch begins 2 minute controlled shutdown at 69° C.

Other Important Notes:

This table lists important information you should be aware of regarding Fabric OS v4.1.1.

Area	Description
Ethernet Port IP addresses	**NOTE:** When a 2109-M12 fails over to its Standby CP for any reason, the IP addresses for the two logical switches move to that CP blade's Ethernet port. This may cause informational ARP address reassignment messages to appear on other switches in the fabric. This is normal behavior, since the association between the IP addresses and MAC addresses has changed.
Fabric OS CLI commands, Failover and Port disable	**NOTE:** Changing port configurations during a failover might cause ports to be in a disabled state. Reissue the command after the failover is complete to bring the port online.
Fabric OS Commands	**Problem:** Under the root account, issuing Fabric OS commands in parallel through scripts could cause the Kernel task to consume excessive memory. **Solution:** When using scripts to issue Fabric OS commands, it is always a good practice to wait for the command to finish before issuing another command.
Fabric OS Commands	The commands moredisable and moreenable were added to the Fabric OS.
Fabric OS Switch Beaconing	**NOTE:** Switch beaconing is not preserved across a failover. If you start beaconing, a failover will cause all lights to stop flashing. **Solution:** If this occurs, reissue the command to resume switch beaconing.

Area	Description
Fabric OS, Switch reboot and Blade Repair	**Problem:** Switch reboot will fail in the 2109 model M12, if there are faulty port blades. **CAUTION: Verify all blades are in working order before performing a switch reboot. Switch reboot is meant to be issued after all repairs are complete. If you do a switch reboot and find a faulty blade, remove the blade and reboot will continue.** **Solution:** Identify and remove the faulty blade using the **slotshow** command to reboot successfully.
Fabric routing, Fabric Manager: domain overlap	**NOTE:** Issuing a **configdefault** followed by reboot or switch disable/enable will cause the fabric to segment due to possible domain overlap. **Solution:** Therefore, before rebooting the Fabric, ensure all switches are properly configured to avoid domain overlap between the logical switches.
Fabric Device Management Interface (FDMI)	**NOTE**: An HBA will be allowed to register even though the originating port is not in the HBA's registered port list. This is intended behavior included in order to test error cases.
Firmware Download	**NOTE:** Please review the Firmware Download section of the Fabric OS Procedures guide before upgrading your firmware.
Firmware Download	**Problem:** During a firmware download, rebooting or power cycling the CPs could cause the compact flash to be corrupted. **CAUTION: Do not attempt to power off the CP board during Firmware Download to avoid high risk of potentially corrupting your flash.**
HA switch reboot failure	**NOTE:** When a switch reboot or a failover occurs before POST is complete, the HA resynchronization will be disrupted. HA will not resynchronize until POST completes. **CAUTION: Allow POST to complete before performing a switch reboot or failover to avoid disruptive failover.**
IP addresses	**CAUTION:** Do not set a switch or CP IP address for the Ethernet interface to 0.0.0.0.
IP Addresses	**NOTE:** Supernetting of IP addresses, also known as CIDR, is not supported in Fabric OS.
License removal	**NOTE:** When a user removes a license from the switch, the feature is not disabled until the switch is rebooted or a switch disable/enable is performed.
LTO 2 Tape Drive Support	When using the LTO 2 Tape Drive, the user must perform the following command on both Fabric OS 3.x and 4.x: switch> portcfggport *port# where drive is plugged into* This will allow the tape drive to function in point to point mode rather than in loop.
OS - Hardware	**NOTE:** Bringing up port blades during a failover could cause the port cards to come up in a disabled state. This is a rare occurrence, and when this happens, redo the port blade bringup after the failover on the 2109 model M12.
Security	**NOTE:** If HTTP_Policy is empty you will not be able to log in and will receive a "Page not found" error. This is expected behavior for this policy.

Area	Description
Security, FCC list	**NOTE:** Adding switches onto the FCC list does not automatically join the switches in a secure fabric. Add the switches to the FCC list and either reset the E-ports or perform a switch disable and enable for the switches to join.
Security, PKICERT utility	**NOTE:** Before using the PKICERT utility to prepare a CSR, please ensure that there are no spaces in the switchnames of any switches in the fabric. The Web site that processes the CSRs and generates the digital certificates does not accept switchnames containing spaces, and any CSRs that do not conform to this requirement will be rejected.
Security, SLAP fail counter and 2 switches	**NOTE:** The SLAP counter is designed to work when all the switches in the fabric are in secure mode. All the switches in the fabric must be in secure mode for accurate SLAP statistics.
Security, SSH login	**NOTE:** To properly connect SSH login, wait for sec mode to complete before rebooting or doing HA failover on the 2109 model M12. If Sec mode is enabled and a reboot occurs before Sec mode completes, SSH login will not connect and will go to the wrong MAC address because the active CP would change after a HA failover.
Security: empty policies	**CAUTION: If telnet, API, and serial port access policies are empty, the user will not be able to talk to the switch.** **Solution:** Contact switch provider for the recovery procedure.
Security: Error counter	**NOTE:** The Telnet security error counter will count each violation as 1 plus any auto retries the telnet software executes.
Security: Secure mode	**NOTE:** When in Secure mode, if you upgrade from Fabric OS version 4.0 to 4.1, then downgrade to Fabric OS version 4.0, and upgrade back to Fabric OS version 4.1, the system prompt will ask the user to reset the secure mode password.
Security: Secure mode, passwd telnet	**CAUTION: Using the passwd telnet command in Secure Mode to change the password results in all sessions using that password to be logged out including the session that changed the session.** **This is expected behavior. The session will terminate if you change the password in secure mode.**
Web Tools and CLI commands	**NOTE:** If you use Web Tools to change the switchName, the 2109 model M12 telnet console prompt will not update to the new name until a new telnet window is opened.
Web tools, Java bug	**Problem:** If a dialog box is displayed from the switch admin window of the Web Tools and the user selects another dialog box from Web Tools, this causes a windows display error. **NOTE:** This is a known defect in Java 1.3 documented at www.java.sun.com, bug ID 4763605. To avoid the display error, open only one dialog box at a time or launch another switch admin session in a separate window.
WWN card FRU repair	**Problem:** If an HA failover or power cycle occurs during a FRU on the WWN card, the 2109 model M12 will become non-operational. **CAUTION: When performing a FRU on a WWN card, complete the FRU procedure before attempting an HA failover or power cycling the chassis.**

Area	Description
Zoning	**NOTE:** To use Zoning in a non-RCS (Reliable Commit Service) mode fabric, that is, in a fabric containing switches with firmware version other than v2.6.x, v3.1 and v4.1, it is recommended that all appropriate Zoning licenses are installed on all the switches in the fabric before attempting to bring a switch in to the fabric. Furthermore, if the Zoning license is to be removed, the user must make sure it is re-installed back properly on the affected switch before attempting **cfgenable** zoning operation. Failure to follow these steps can cause inconsistency of Zoning configuration on the affected switches should a zoning operation be attempted from a remote switch in the fabric. On the affected switches an error message will appear on the console or telnet session (can also be seen by doing **errShow**, **errDump**) indicating that zoning license was missing.
Zoning	**Problem:** Domain 0 in a zoning configuration file is illegal but was not previously enforced. **NOTE:** Prior to upgrading a switch to 4.1, please ensure that the fabric's zoning configuration does not contain the Domain ID 0 used for zoning. This is specific only to 4.x switches.

Defects Closed In Fabric OS 4.1.1a

Defects Closed In Fabric OS v4.1.1a		
Defect ID	**Severity**	**Description**
DEFECT000026554	Critical	Summary: 2109 model F32 switch port is left INSYNC after a reboot of the array Symptom: When a loop capable device negotiates to the F-port briefly, and NOS happens, the switch port does not complete port initialization at LIP phase. The port is left in the IN_SYNC state. Solution: Enable the LPSM_OPEN_INIT_RCVD interrupt when appropriate, to prevent the port from hanging during port initialization.
DEFECT000026397	High	Summary: Incorrect behavior in FOS 4.0.2c after ABTS is sent to the Name Server Symptom: When HBA accepts first RSCN, and then communicates to the name server to get new information. Another RSCN is sent, which the HBA accepts and sends ABTS to the name server for the previous query. The name server accepts but then sends the reply to the query that's not needed. Solution: Drop the iu if the sequence has been aborted.
DEFECT000026431	High	Summary: The servers in the SAN failed to recover any drives when many drivers are power up at the same time. Symptom: In a fabric with zoning turned on, the LTO tape subsystem was powered down. After the SAN stabilized, the LTO was powered up. After 8 to 10 minutes, the servers that connected to the switch

Defects Closed In Fabric OS v4.1.1a		
Defect ID	**Severity**	**Description**
		(Fabric OS v4.0.0x) with the tape subsystem successfully recovered all drives. However, the servers that connected to other switches in the SAN failed to recover any drives. Solution: From the traces, it shows that many PLOGIs were sent from the server after receiving the RSCNs, but only three of the PLOGI ACC were received back, other ACC to the PLOGI were dropped. The PLOGI and ACC were trapped by different filters. The solution is to update and synchronize the different filters to avoid this issue.
DEFECT000026615	High	Summary: CP timeout during firmware upgrade Symptom: During the firmware upgrade from Fabric OS 4.0.x to 4.1.1, the active control processor (CP) with 4.1.1 resets the other CP while the other CP is in the middle of upgrading firmware. This reset either corrupts the other CP's PROM or causes failure to the other CP's upgrade process. Solution: Use the same time window for detecting heartbeat as Fabric OS 4.0.x.
DEFECT000033165	High	Summary: Firmware download failed on 2109 model F32 when using Webtools to upgrade firmware from v4.0.2c to v4.1.1 Symptom: Using Web Tools to upgrade firmware from v4.0.2c to v4.1.1 causes ASSERT panic. Web Tools cannot abort the firmware download after the switch reboots. Subsequently, the user cannot restart another firmware download. Solution: In single CP case, ASSERT is not needed. Removed the ASSERT.