UNH-IOL
FIBRE CHANNEL CONSORTIUM

FCoE Initialization Protocol (FIP) Snooping Test Suite
Version 1.0

Technical Document

Last Updated: August 1, 2012

Fibre Channel Consortium
InterOperability Laboratory
University of New Hampshire

121 Technology Drive, Suite 2
Durham, NH 03824
Phone: (603) 862-0701
Fax: (603) 862-4181
http://www.iol.unh.edu/consortiums/fc

Table of Contents

Modification Record

August 1, 2012 (Version 1.0) Dan Shea

Acknowledgements

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite.

Dan Shea	University of New Hampshire
Mikkel Hagen	University of New Hampshire

Introduction

Overview

The University of New Hampshire's InterOperability Laboratory (IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard. This suite of tests has been developed to help vendors evaluate the functioning of their Fibre Channel over Ethernet based products. Rather, they provide one method to isolate problems within a Fibre Channel over Ethernet device. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with all other Fibre Channel over Ethernet devices. However, combined with satisfactory operation in the IOL's semi-production environment, these tests provide a reasonable level of confidence that the Device Under Test (DUT) will function well in most multi-vendor Fibre Channel over Ethernet environments.

Test Number and Title: The test number is given based on the order of the test within the test group. Groups are arranged according to similar test setups or similar observable results. The title is a basic description of the test.

Purpose: The purpose is a short statement describing what the test attempts to achieve. The test is written at the functional level.

References: This section specifies all reference material that might be helpful in understanding the test methodology and/or test results.

Resource Requirements: The requirements section specifies the test hardware and/or software needed to perform the test. This is generally expressed in terms of minimum requirements, however in some cases specific equipment manufacturer/model information may be provided.

Last Modification: This specifies the date of the last modification to this test.

Discussion: The discussion covers the assumptions made in the design or implementation of the test, as well as known limitations. Other items specific to the test are covered here as well.

Test Setup: The setup section describes the initial configuration of the test environment. Small changes in the configuration should not be included here, and are generally covered in the test procedure section (next).

Procedure: The procedure section of the test description contains the systematic instructions for carrying out the test. It provides a cookbook approach to testing, and may be interspersed with observable results.

Observable Results: This section lists the specific observables that can be examined by the tester in order to verify that the DUT is operating properly. When multiple values for an observable are possible, this section provides a short discussion on how to interpret them. The determination of a pass or fail outcome for a particular test is generally based on the successful (or unsuccessful) detection of a specific observable.

Possible Problems: This section contains a description of known issues with the test procedure, which may affect test results in certain situations. It may also refer the reader to test suite appendices and/or other external sources that may provide more detail regarding these issues.

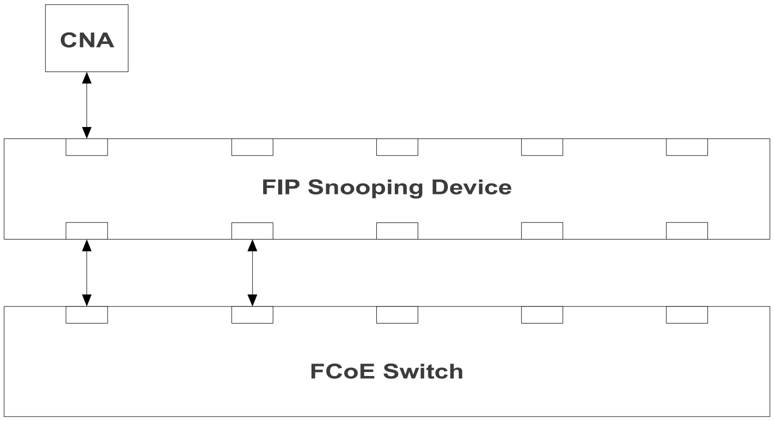
References

The following documents are referenced in this text:

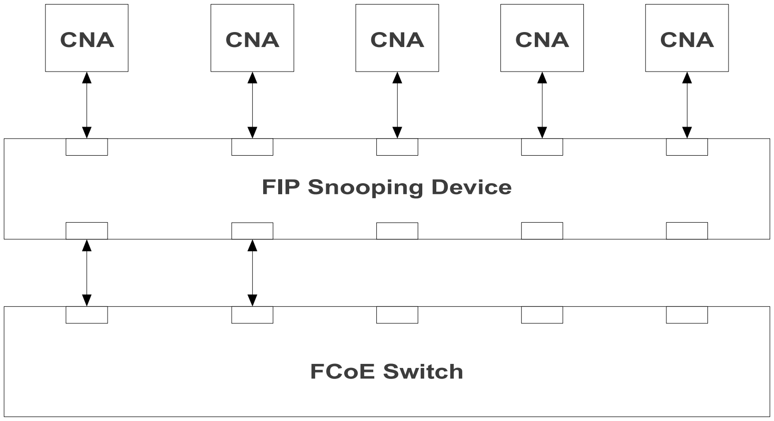
- ANSI X3T11/Project 1871-D/Rev. 2.00 Fibre Channel Backbone 5 FC-BB-5 (hereafter referred to as “FC-BB-5”)

Test Setups

Test Setup 1: The Initiator is connected to the FIP Snooping Device. The The FIP Snooping Device is then connected to the FCoE Switch.



Test Setup 2: The Initiators are connected to the FIP Snooping Device. The The FIP Snooping Device is then connected to the FCoE Switch.



Group 1: Screening

Overview: These tests are designed to verify basic interoperability of different Initiators with the FCF when going through a FIP snooping device. The following tests examine the behavior of a FIP snooping device's ability to properly forward FCoE traffic from an Initiator to the FCF.

Test 1.1: Single ENode to Single FCF in a VLAN

Purpose: To verify that a single initiator is able to properly log into an FCF on the same VLAN through the FIP snooping device.

References:

[1] FC-BB-5 – Sub-Annex C.1

Resource Requirements:

- One FCoE Initiator.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: The FCF is tested in a paired setup with each Initiator. The FIP snooping device is configured to monitor FCoE traffic on a configured VLAN ID. The FCoE Switch is configured to provide the same VLAN ID to the end node. It is then verified that the Initiator is still logged into the FCF while the FIP snooping device reports the Initiator and the FCF as being logged in.

Test Setup: *Test Setup 1.* The Initiator is connected to the FCF through the FIP snooping device. The Initiator and the FCF are powered on.

Procedure:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002.
2. Configure the FCoE Switch to provide a VLAN ID of 1002 to the end node via VLAN Discovery.

Observable Results:

- Verify that the Initiator and the FCF are logged into the FIP snooping device and appear in the name server of the FIP snooping device.

Possible Problems: None.

Group 2: FIP Snooping

Overview: These tests observe a FIP snooping device's ability to properly forward FCoE traffic on a network while conforming to the FC-BB-5 standard.

Test 2.1: Multiple ENodes to Single FCF in a VLAN

Purpose: To verify that multiple initiators are able to properly log into an FCF on the same VLAN through the FIP snooping device.

References:

[1] FC-BB-5 – Sub-Annex C.1

Resource Requirements:

- Two or more FCoE Initiators.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: The FCF is tested in a test setup with all Initiators. The FIP snooping device is configured to monitor FCoE traffic on a configured VLAN ID. The FCoE Switch is configured to provide the same VLAN ID to the end nodes. It is then verified that all Initiators are still logged into the FCF while the FIP snooping device reports all Initiators and the FCF as being logged in.

Test Setup: *Test Setup 2.* The Initiators are connected to the FCF through the FIP snooping device. The Initiators and the FCF are powered on.

Procedure:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002.
2. Configure the FCoE Switch to provide a VLAN ID of 1002 to the end nodes via VLAN Discovery.

Observable Results:

- Verify that the Initiators and the FCF are logged into the FIP snooping device and appear in the name server of the FIP snooping device.

Possible Problems: None.

Test 2.2: Single ENode with Multiple VN_Port Sessions to Single FCF

Purpose: To verify that multiple virtual N_Ports on a single initiator are able to properly log into an FCF through the FIP snooping device.

References:

[1] FC-BB-5 – Sub-Annex C.1

Resource Requirements:

- One FCoE Initiator.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: The VN_Ports on the Initiator are tested in a test setup involving the one Initiator going through a FIP snooping device to the FCF. The FIP snooping device is configured to monitor FCoE traffic on a configured VLAN ID. The FCoE Switch is configured to provide the same VLAN ID to the VN_Ports. It is then verified that all VN_Ports on the Initiator are still logged into the FCF while the FIP snooping device reports all VN_Ports and the FCF as being logged in.

Test Setup: *Test Setup 1.* The Initiator is connected to the FCF through the FIP snooping device. The Initiator and the FCF are powered on.

Procedure:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002.
2. Create four virtual N_Ports on the Initiator.
3. Configure the FCoE Switch to provide a VLAN ID of 1002 to the VN_Ports via VLAN Discovery.

Observable Results:

- Verify that the VN_Ports and the FCF are logged into the FIP snooping device and appear in the name server of the FIP snooping device.

Possible Problems: None.

Test 2.3: Multiple ENode-FCF Combinations over Multiple FC Fabrics

Purpose: To verify that multiple initiators are able to properly log into an FCF through the FIP snooping device across multiple VLANs.

References:

[1] FC-BB-5 – Sub-Annex C.1

Resource Requirements:

- Two or more FCoE Initiators.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: The use of multiple FC fabrics are tested in a test setup involving all Initiators going through a FIP snooping device to the FCF. The FIP snooping device is configured to monitor FCoE traffic on two configured VLAN IDs. The FCoE Switch is configured to provide the same two VLAN IDs to the Initiators. It is then verified that all Initiators are logged into the FCF on both VLANs while the FIP snooping device reports all Initiators and the FCF as being logged in across both VLANs.

Test Setup: *Test Setup 2.* The Initiators are connected to the FCF through the FIP snooping device. The Initiators and the FCF are powered on.

Procedure:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002 and VLAN 1279.
2. Configure the FCoE Switch to provide VLAN IDs of 1002 and 1279 to the Initiators via VLAN Discovery.

Observable Results:

- Verify that the Initiators and the FCF are logged into the FIP snooping device across all VLANs and appear in the name server of the FIP snooping device.

Possible Problems: None.

Test 2.4: Manually Configure FCFs

Purpose: To verify that multiple initiators are able to properly log into an FCF through the FIP snooping device when the FIP snooping device is manually configured to accept a specific FCF MAC Address.

References:

[1] FC-BB-5 – Sub-Annex C.2

Resource Requirements:

- Two or more FCoE Initiators.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: When a FIP snooping device is set to manually accept FCF MAC Addresses, the FIP snooping device must only accept MAC addresses equal to an accepted MAC Address in its internal table. For testing, the FIP snooping device should be configured to monitor FCoE traffic on a particular VLAN ID and manually accept provided FCF MAC Addresses. The FCF MAC is registered with the FIP snooping device. The FCoE Switch is configured to provide the same VLAN ID to the Initiators.

Test Setup: *Test Setup 2.* The Initiators are connected to the FCF through the FIP snooping device. The Initiators and the FCF are powered on.

Procedure:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002. Disable automatic FCF MAC entries and manually insert the MAC Address of the FCF.
2. Configure the FCoE Switch to provide VLAN ID 1002 to the Initiators via VLAN Discovery.

Observable Results:

- Verify that the Initiators and the FCF are logged into the FIP snooping device and appear in the name server of the FIP snooping device.

Possible Problems: None.

Test 2.5: Disallow FCoE Traffic from Rogue ENode/FCF

Purpose: To verify that a rogue initiator does not log into an FCF through the FIP snooping device. It is also verified that initiators do not log into a rogue FCF when a set of allowed FCF MAC Addresses have been manually registered with the FIP snooping device.

References:

[1] FC-BB-5 – Sub-Annex C.6
[2] FC-BB-5 – Sub-Annex D.4

Resource Requirements:

- Two or more FCoE Initiators.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: When a FIP snooping device is set to manually accept FCF MAC Addresses, the FIP snooping device must only accept MAC addresses equal to an accepted MAC Address in its internal table. If an FCF has a MAC Address not present in the table, such an FCF should not be able to establish virtual links with the Initiators on the network. For testing, the FIP snooping device should be configured to monitor FCoE traffic on a particular VLAN ID and manually accept provided FCF MAC Addresses. A MAC Address not identical to the FCF MAC is registered with the FIP snooping device. The FCoE Switch is configured to provide the same VLAN ID to the Initiators. An Initiator is connected to a port on the FIP snooping device which has not been configured for the VLAN being used.

Test Setup: *Test Setup 2.* The Initiators are connected to the FCF through the FIP snooping device. The Initiators and the FCF are powered on.

Procedure:

Part A:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002.
2. Connect one Initiator to a port which has not been configured for VLAN 1002. Connect all other Initiators to ports configured for VLAN 1002.
3. Configure the FCoE Switch to provide VLAN ID 1002 to the Initiators via VLAN Discovery.

Part B:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002. Disable automatic FCF MAC entries and manually insert a MAC Address not identical to the MAC Address of the FCF, clearing any additional entries in the table if they exist.
2. Configure the FCoE Switch to provide VLAN ID 1002 to the Initiators via VLAN Discovery.

Observable Results:

- **Part A:** Verify that the Initiator connected to the port not enabled for VLAN 1002 did not log into the FIP snooping device. Also verify that all other Initiators are logged into the FIP snooping device and appear in the name server of the FIP snooping device.
- **Part B:** Verify that the FCF is not logged into the FIP snooping device.

Possible Problems: None.

Test 2.6: FCF-to-ENode Ports Reject FCF Source MAC

Purpose: To verify that the FIP snooping device rejects FCoE traffic sent to an FCF when the destination port is an ENode port and the MAC Address is equal to the FCF Source MAC Address.

References:

[1] FC-BB-5 – Sub-Annex D.4

Resource Requirements:

- One FCoE Initiator.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: When a FIP snooping device receives a frame from a known ENode port with a source MAC equal to a known FCF, the FIP snooping device should discard the frame. For testing, the FIP snooping device should be configured to monitor FCoE traffic on a particular VLAN ID and automatically accept provided FCF MAC Addresses. The FCoE Switch is configured to provide the same VLAN ID to the Initiator.

Test Setup: *Test Setup 1.* The Initiator is connected to the FCF through the FIP snooping device. The Initiator and the FCF are powered on.

Procedure:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002.
2. Configure the FCoE Switch to provide a VLAN ID of 1002 to the end node via VLAN Discovery.
3. Configure the Initiator to transmit FCoE traffic with a source MAC equal to the FCoE Switch.
4. Transmit FCoE traffic from the Initiator to the FCoE Switch.

Observable Results:

- Verify that the FCF does not act on any FCoE traffic with the FCF source MAC transmitted from the Initiator and that the FIP snooping device discards any FCoE traffic with the FCF source MAC from the Initiator.

Possible Problems: None.

Test 2.7: ENode/FCF Port Functionality

Purpose: To verify that the FIP snooping device rejects FCF traffic on an ENode-to-FCF port and ENode traffic on an FCF-to-ENode port.

References:

[1] FC-BB-5 – Sub-Annex D.4

Resource Requirements:

- One FCoE Initiators.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: An ENode-to-FCF port should only accept traffic from a known ENode to a known FCF. Likewise, an FCF-to-ENode port should only accept traffic from a known FCF to a known ENode. All other forms of traffic should be discarded. For testing, the FIP snooping device should be configured to monitor FCoE traffic on a particular VLAN ID. The FCoE Switch is configured to provide the same VLAN ID to the Initiator.

Test Setup: *Test Setup 1.* The Initiator is connected to the FCF through the FIP snooping device. The Initiator and the FCF are powered on.

Procedure:

Part A:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002.
2. Configure the FCoE Switch to provide a VLAN ID of 1002 to the end node via VLAN Discovery.
3. Transmit FCoE traffic from the Initiator to the FCoE Switch. The Destination MAC of the FCoE traffic should not be equal to the FCoE Switch's MAC Address.

Part B:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002.
2. Configure the FCoE Switch to provide a VLAN ID of 1002 to the end node via VLAN Discovery.
3. Transmit FCoE traffic from the FCoE Switch to the Initiator. The Destination MAC of the FCoE traffic should not be equal to the Initiator's MAC Address.

Observable Results:

- **Part A:** Verify that the FIP snooping device discards all FCoE traffic received from the Initiator.
- **Part B:** Verify that the FIP snooping device discards all FCoE traffic received from the FCoE Switch.

Possible Problems: None.

Test 2.8: VN_Port MACs Allowed in FPMA Mode

Purpose: To verify that, when the FIP snooping device is in FPMA mode, all source MACs which match the VN_Port MACs are allowed and that all other source MACs whose most significant 24 bits match the fabric's FC-MAP are discarded and the MAC addresses are not learnt.

References:

[1] FC-BB-5 – Sub-Annex D.6

Resource Requirements:

- Two or more FCoE Initiators.
- One FIP snooping device.
- One FCoE Switch.
- Monitor capable of capturing Fibre Channel over Ethernet traffic.

Modification Record: August 1, 2012

Discussion: Misconfiguration or network issues may cause multiple VN_Ports to utilize the same MAC address, leading to network failures such as the undetected corruption of data. FPMAs make it possible to assign allowed MAC addresses across VN_Ports by learning them through FIP and FCoE traffic, discarding all other frames in which the most significant 24 bits of the source MAC address match the fabric's FC-MAP. For testing, the FIP snooping device should be configured to monitor FCoE traffic on a particular VLAN ID. The FCoE Switch is configured to provide the same VLAN ID to the Initiator.

Test Setup: *Test Setup 2.* The Initiators are connected to the FCF through the FIP snooping device. The Initiators and the FCF are powered on.

Procedure:

Part A:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002. Set the FIP snooping device to FPMA mode and allow all traffic from the Initiators.
2. Configure the FCoE Switch to provide a VLAN ID of 1002 to the end node via VLAN Discovery.

Part B:

1. Configure the FIP snooping device to monitor FCoE traffic on VLAN 1002. Set the FIP snooping device to FPMA mode and set the FC-MAP to 00:01:02:00:00:00.
2. Configure the FCoE Switch to provide a VLAN ID of 1002 to the end node via VLAN Discovery.

Observable Results:

- **Part A:** Verify that the FIP snooping device properly forwards all FCoE traffic.
- **Part B:** Verify that the FIP snooping device discards the FCoE traffic and does not learn the MAC addresses.

Possible problems: None.