iSCSI Consortium
CHAP Test Suite
For iSCSI Targets

Version 0.1

Last Update: June 16, 2003

iSCSI Consortium
InterOperability Laboratory
Research Computing Center
University of New Hampshire
http://www.iol.unh.edu

121 Technology Drive Suite 2
Durham, NH 03824-3525
Phone: (603) 862-1908
Fax: (603) 862-4181

MODIFICATION RECORD

1. Currently on Version 0.1. Version 1.0 is awaiting publication of iSCSI RFC

ACKNOWLEDGMENTS

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

David Woolf 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 implementers evaluate the functioning of their iSCSI products. The tests do not determine if a product conforms to the iSCSI draft standard, nor are they purely interoperability tests. Rather, they provide one method to isolate problems within an iSCSI device. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other iSCSI 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 multivendor iSCSI environments.

Organization of Tests

The tests contained in this document are organized to simplify the identification of information related to a test and to facilitate in the actual testing process. Each test contains an identification section that describes the test and provides cross reference information. The detailed section discusses the background information and specifies how the test is to be performed. Tests are grouped in order to reduce setup time in the lab environment. Each test contains the following information:

Test Label

The Label associated with each test is a title that is used to refer to the test. The attached number is an internal reference number dealing with an internal reference to 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

The references section lists cross references to the iSCSI draft standard and other documentation that might be helpful in understanding and evaluating the test and results.

Resource Requirements

The requirements section specifies the software, hardware, and test equipment that will be needed to perform the test. The items contained in this section are special test devices, software that must reside on the DUT, or other facilities which may not be available on

all devices.

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.

Test Setup
The setup section describes in detail the configuration of the test environment and includes a block diagram for clarification as well as information such as the interconnection of devices, what monitoring equipment should capture, what the generation equipment should send, and any other configuration information vital to carrying out the test. Small changes in the configuration should be included in the test procedure.

Procedure
The procedure section of the test description contains the step-by-step instructions for carrying out the test. It provides a cookbook approach to testing, and will often be interspersed with observable results.

Observable Results
The observable results section lists observables that can be examined by the tester to verify that the DUT is operating properly. When multiple values are possible for an observable, this section provides a short discussion on how to interpret them. Note that complete delineation between the observables in the **Procedure** and **Observable Results** is virtually impossible. As such a careful note should be made of the requirements in both sections. In certain cases, it may be necessary to modify certain steps in the **Procedure** section while doing the actual tests so as to be able to perform the tests. In such cases, the modifications will be noted in the summary report.

Possible Problems
This section provides some clues to look for if the test does not yield the expected results.

REFERENCES

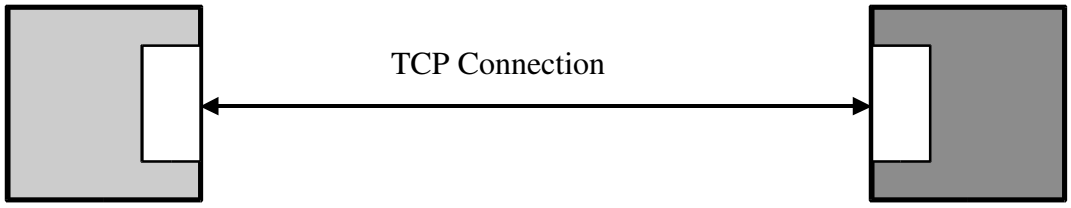
The following documents are referenced in this text:

IETF IPS Working Group iSCSI draft 20

TEST SETUPS

The following test setups are used in this test suite:

Test Setup 1:



Testing Station/ Monitor DUT

TABLE OF CONTENTS

Test #1.1: CHAP_A Valid Value

Purpose: To see that the DUT properly responds to a received CHAP_A key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:34:20 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
• Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5.

Observable Results:
• Verify that the DUT responds the the received CHAP_A key with CHAP_A=5.
· Verify that the DUT transmits a Login Response PDU with the CHAP_C=C and CHAP_I=I key=value pairs.
· Verify that the values for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.

Possible Problems: There is no requirement that CHAP_A, CHAP_I, and CHAP_C be

in the same Login Response PDU.

Test #1.2: CHAP_A Valid Value In List

Purpose: To see that the DUT properly responds to a received CHAP_A key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:34:27 2003

Discussion: For CHAP the initiator MUST use: CHAP_A= Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=1,3,5,9.

Observable Results:
· Verify that the DUT recognizes that the required value of 5 is present
· Verify that the DUT responds the the received CHAP_A key with CHAP_A=5.
· Verify that the DUT transmits a Login Response PDU with the CHAP_C=C and CHAP_I=I key=value pairs.
· Verify that the values for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number. CHAP_C should be a binary value not exceeding 1024 bytes.

Possible Problems: None.

Test #1.3: CHAP_A Invalid Value

Purpose: To see that the DUT properly responds to a received CHAP_A key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:34:35 2003

Discussion: For CHAP the initiator MUST use: CHAP_A= Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=WickedGood.

Observable Results:
· Verify that the DUT recognizes that the required value of 5 is not present, and the DUT transmits a Login Reject with 'Authentication failure' as the Status code.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #1.4: CHAP_A Valid Value Not In List

Purpose: To see that the DUT properly responds to a received CHAP_A key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:34:42 2003

Discussion: For CHAP the initiator MUST use: CHAP_A= Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=1,3,7,9.

Observable Results:
· Verify that the DUT recognizes that the required value of 5 is not present, and the DUT transmits a Login Reject with 'Authentication Failure' as the Status code.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #1.5: CHAP_A Out of Order

Purpose: To see that the DUT properly responds when CHAP_A is received out of order.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:34:49 2003

Discussion: For CHAP the initiator MUST use: CHAP_A= Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station. .
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_I=I, CHAP_C=C, CHAP_A=5.

Observable Results:
· Verify that the DUT recognizes that this violates the step definitions and and the DUT transmits a Login Reject with 'Initiator Error' or 'Missing Parameter' as the Status code.

Possible Problems: The DUT may transmit a Login Reject with status of 'Authentication Failure'. This is acceptable.

Test #1.6: CHAP_A Out of Order

Purpose: To see that the DUT properly responds when CHAP_A is not received.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:34:57 2003

Discussion: For CHAP the initiator MUST use: CHAP_A= Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_I=I, CHAP_C=C.

Observable Results:
· Verify that the DUT recognizes that this violates the step definitions and and the DUT transmits a Login Reject with 'Initiator Error' or 'Missing Parameter' as the Status code.

Possible Problems: The DUT may transmit a Login Reject with status of 'Authentication Failure'. This is acceptable.

Test #2.1: CHAP_I Valid Value

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:35:04 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer CHAP_N, CHAP_R, CHAP_I, CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary

value not exceeding 1024 bytes.
· Verify that the DUT responds to the received CHAP_I and CHAP_C with a correct CHAP_R, and also offers a valid CHAP_N. CHAP_N should be a text string between 1 and 255 bytes in length. CHAP_R should be a binary value of 16 bytes, if using MD5 hash algorithm.

Possible Problems: None.

Test #2.2: CHAP_I Invalid Value

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:35:11 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer CHAP_N, CHAP_R, CHAP_I as a string and CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary

value not exceeding 1024 bytes.
· Verify that the DUT responds to the received CHAP_I with Login Reject 'Authentication Failure' status.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #2.3: CHAP_I No Value

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:35:18 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer CHAP_N, CHAP_R, CHAP_I with no value and CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary

value not exceeding 1024 bytes.
· Verify that the DUT responds to the received CHAP_I key with Login Reject 'Authentication Failure' status.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #2.4: CHAP_I Too Big Value

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:35:25 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer CHAP_N, CHAP_R, CHAP_I which has a value which is 2 bytes long, and CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary

value not exceeding 1024 bytes.
· Verify that the DUT responds to the received CHAP_I key with Login Reject 'Authentication Failure' status.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #2.5.1: CHAP_I Out of Order

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:35:35 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5, CHAP_I.

Observable Results:
· Verify that the DUT responds to the received CHAP_I key with Login Reject 'Authentication Failure' status.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #2.5.2: CHAP_I Out of Order

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:35:42 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer CHAP_I and CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary

value not exceeding 1024 bytes.
· Verify that the DUT does not respond to the received CHAP_I and CHAP_C values by sending CHAP_N and CHAP_R, as this would violate the step definition. The DUT can choose to send an empty Login Response, indicating that it is waiting for the Testing Station to transmit CHAP_N and CHAP_R to complete the step.

Possible Problems: The DUT may transmit a Login Reject. Although none of the behavior described in the procedure is illegal, a Login Reject is acceptable.

Test #2.6.1: CHAP_I Reused on Second Connection

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:35:52 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer CHAP_N, CHAP_R, and CHAP_I and CHAP_C (8 bytes) to request Target Authentication.
· The DUT is expected to respond with CHAP_N and CHAP_R. Move on the Operational Parameter Negotiation then to Full Feature Phase operations.
· Open a second connection to the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer

AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer the same CHAP_I and a new CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the DUT accepts each instance of CHAP_I received from the Testing Station.

Possible Problems: None.

Test #2.6.2: CHAP_I Different on Second Connection

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Tue May 27 09:15:57 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the DUT and the Testing Station with the same CHAP secret.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer CHAP_N, CHAP_R, and CHAP_I and CHAP_C (8 bytes) to request Target Authentication.
· The DUT is expected to respond with CHAP_N and CHAP_R. Move on the Operational Parameter Negotiation then to Full Feature Phase operations.
· Open a second connection to the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with,

CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer a new CHAP_I and a new CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the DUT accepts each instance of CHAP_I received from the Testing Station.

Possible Problems: None.

Test #2.7.1: CHAP_I Reflected

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:36:01 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station. t.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer the same CHAP_I as the DUT and a new CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the DUT accepts each instance of CHAP_I received from the Testing Station.

Possible Problems: None.

Test #2.7.2: CHAP_I Reflected on Second Connection

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair.

Reference: 11.1.4

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:36:10 2003

Discussion: For CHAP the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=A CHAP_I=I CHAP_C=C. Where A is one of A1,A2... that were proposed by the initiator. At this point if the initiator requires Target Authentication it should transmit CHAP_N, CHAP_R, CHAP_I, and CHAP_C. The Target is expected to reply with CHAP_N and a CHAP_R which matches the received CHAP_I and CHAP_C. The CHAP_I key should be a 1 byte hex value.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer CHAP_I and CHAP_C (8 bytes) to request Target Authentication.
· The DUT is expected to respond with CHAP_N and CHAP_R. Move on the Operational Parameter Negotiation then to Full Feature Phase operations.
· Open a second connection to the DUT.
· During the Security Negotiation Phase of Login, the Testing Station should offer

AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer the same CHAP_I used by the DUT on the first connection and a new CHAP_C (8 bytes) to request Target Authentication.

Observable Results:
· Verify that the DUT accepts each instance of CHAP_I received from the Testing Station, and does not transmit Login Reject.

Possible Problems: None.

Test #3.1: CHAP_C Reused

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:36:34 2003

Discussion: The Challenge Value MUST be changed each time a Challenge is sent.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a session of SessionType=Normal to the DUT. After the first connection reaches the Full Feature Phase, the Testing Station should start a second connection.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.

Observable Results:
· Verify that the DUT uses different values for CHAP_C on each connection.

Possible Problems: This item is not testable if the DUT does not support multiple connections.

Test #3.2: CHAP_C Big Value

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: 11.1.4, RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:36:42 2003

Discussion: The Challenge Value is binary value between 1 and 1024 bytes.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should respond with valid values for CHAP_N, CHAP_R, CHAP_I. CHAP_C should also be offered, formatted as a binary, for size 1024 bytes.

Observable Results:
· Verify that the DUT does not end the negotiation but rather responds with valid and accurate values for CHAP_N and CHAP_R.

Possible Problems: None.

Test #3.3: CHAP_C Small Value

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: 11.1.4, RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:36:48 2003

Discussion: The Challenge Value is binary value between 1 and 1024 bytes.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station. et.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should respond with valid values for CHAP_N, CHAP_R, CHAP_I. CHAP_C should also be offered, formatted as a binary, for size 1 byte.

Observable Results:
· Verify that the DUT does not end the negotiation but rather responds with valid and accurate values for CHAP_N and CHAP_R.

Possible Problems: None.

Test #3.4: CHAP_C Too Big Value

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: 11.1.4, RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:36:55 2003

Discussion: The Challenge Value is binary value between 1 and 1024 bytes.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should respond with valid values for CHAP_N, CHAP_R, CHAP_I. CHAP_C should also be offered formatted as a binary with a length of 1028.

Observable Results:
· Verify that the DUT end the negotiation with a Login Reject with status 'Authentication Failure'.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #3.5: CHAP_C Out of Order

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: 11.1.4, RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:37:02 2003

Discussion: The Challenge Value is binary value between 1 and 1024 bytes.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5 and CHAP_C. CHAP_C should be formatted as a binary and be 8 bytes long.

Observable Results:
· Verify that the DUT end the negotiation with a Login Reject with status 'Authentication Failure'.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #3.6: CHAP_C Receive Reused

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:37:09 2003

Discussion: The Challenge Value MUST be changed each time a Challenge is sent.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a session of SessionType=Normal to the DUT. After the first connection reaches the Full Feature Phase, the Testing Station should start a second connection.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· On each connection the Testing Station should offer appropriate CHAP_N and CHAP_R responses. The DUT should offer the different CHAP_I and identical CHAP_C values on each connection. These values should not be the same as the values offered by the DUT.

Observable Results:
· Verify that the DUT transmits Login Reject with 'Authentication Failure' Status.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable. This item is not testable if the DUT does not support multiple connections.

Test #3.7: CHAP_C Reflected

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:37:18 2003

Discussion: The Challenge Value MUST be changed each time a Challenge is sent.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· The Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer appropriate CHAP_N and CHAP_R responses. The Testing Station should offer a different CHAP_I value and should reflect the CHAP_C values provided by the DUT.

Observable Results:
· Verify that the DUT transmits Login Reject with 'Authentication Failure' Status.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #3.8: CHAP_C Reflected on Second Connection

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:37:26 2003

Discussion: The Challenge Value MUST be changed each time a Challenge is sent.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a session of SessionType=Normal to the DUT. After the first connection reaches the Full Feature Phase, the Testing Station should start a second connection.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· The Testing Station should respond with valid values for CHAP_R and CHAP_N on each connection. The Testing Station should offer the same values for CHAP_I and CHAP_C as offered by the DUT on the first connection, as the Testing Stations values for CHAP_I and CHAP_C on the second connection. Thus the DUT's CHAP_I and CHAP_C from the first connection are reflected onto the second connection. On the first connection the DUT should offer random, valid CHAP_I and CHAP_C to the DUT.

Observable Results:
· Verify that the DUT transmits Login Reject with status 'Authentication Failure'.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable. This item is not testable if the DUT does not support multiple connections.

Test #3.9: CHAP_C New on Second Connection

Purpose: To see that the DUT properly responds to a received CHAP_C key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:37:35 2003

Discussion: The Challenge Value MUST be changed each time a Challenge is sent.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a session of SessionType=Normal to the DUT. After the first connection reaches the Full Feature Phase, the Testing Station should start a second connection.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· The Testing Station should respond with valid values for CHAP_R and CHAP_N CHAP_I and CHAP_C on each connection.

Observable Results:
· Verify that the DUT transmits valid CHAP_N and CHAP_R responses and moves on to Operational Stage Negotiation.

Possible Problems: This item is not testable if the DUT does not support multiple connections.

Test #4.1: CHAP_N Invalid

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:37:44 2003

Discussion: The CHAP_N value is defined as a string.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· The Testing Station should respond with valid values for CHAP_R, CHAP_I and CHAP_C. CHAP_N should also be included, but be a number instead of a string.

Observable Results:
· Verify that the DUT accepts the received CHAP_N.

Possible Problems: None.

Test #4.2: CHAP_N Big

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:37:52 2003

Discussion: The CHAP_N key is limited to 255 bytes in size.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· The Testing Station should respond with valid values for CHAP_R, CHAP_I and CHAP_C. CHAP_N should also be included formatted as a string 255 bytes in length.

Observable Results:
· Verify that the DUT transmits valid CHAP_N and CHAP_R in response, and does not transmit Login Reject.

Possible Problems: None.

Test #4.3: CHAP_N Small

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:38:01 2003

Discussion: The CHAP_N should be between 1 and 255 bytes in size.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· The Testing Station should respond with valid values for CHAP_R, CHAP_I and CHAP_C. CHAP_N should also be included formatted as a string 1 byte in length.

Observable Results:
· Verify that the DUT transmits valid CHAP_N and CHAP_R in response, and does not transmit Login Reject.

Possible Problems: None.

Test #4.4: CHAP_N Too Big

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:38:06 2003

Discussion: The CHAP_N should be between 1 and 255 bytes in size.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station. .
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· The Testing Station should respond with valid values for CHAP_R, CHAP_I and CHAP_C. CHAP_N should also be included formatted as a string 256 bytes long.

Observable Results:
· Verify that the DUT transmits Login Reject with status of 'Authentication Failure'.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable. The DUT may require that the CHAP_N key be configured before Authentication is attempted. In this case, if the DUT will not accept a configuration with CHAP_N > 255 bytes, this item is not testable.

Test #4.5: CHAP_N Out of Order

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:38:15 2003

Discussion: The CHAP_N value is sent after CHAP_C and CHAP_I are received.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5 and CHAP_N where N is a valid value.

Observable Results:
· Verify that the DUT transmits Login Reject with status of 'Authentication Failure'.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable.

Test #4.6: CHAP_N Identical

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:38:23 2003

Discussion: There is no requirement that the CHAP_N value cannot be reused, reflected, changed, or unchanged.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a session of SessionType=Normal to the DUT. After the first connection reaches the Full Feature Phase, the Testing Station should start a second connection.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· On each connection the Testing Station should offer appropriate CHAP_N, CHAP_R, CHAP_I, and CHAP_C. CHAP_N should be the same on each connection. CHAP_I shoul dbe different on each connection. The DUT should respond with valid values for CHAP_N and CHAP_R. The Testing Station should offer identical CHAP_N values on each connection. These values should not be the same as the values offered by the DUT.

Observable Results:
· Verify that the DUT transmits valid CHAP_N and CHAP_R in response, and does not transmit Login Reject.

Possible Problems: This item is not testable if the DUT does not support multiple connections.

Test #4.7: CHAP_N Reflect

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:38:33 2003

Discussion: There is no requirement that the CHAP_N value cannot be reused, reflected, changed, or unchanged.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a session of SessionType=Normal to the DUT. After the first connection reaches the Full Feature Phase, the Testing Station should start a second connection.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· On each connection the Testing Station should offer appropriate CHAP_N, CHAP_R, CHAP_I, CHAP_C. The DUT should offer the appropriate CHAP_N and CHAP_R values. The Testing Station should offer different CHAP_N values on each connection. One of these values should be the same as the value offered by the DUT.

Observable Results:
· The DUT may choose to transmit Login Reject to the reflected CHAP_N. The DUT may choose to accept the reflected CHAP_N, if it has a weak implementation of CHAP.

Possible Problems: An implementation may choose to accept only CHAP_N values it has been configured to accept. This would be a strong implementation of CHAP security. An implementation also could choose to accept any CHAP_N value. This would be a weak implementation of CHAP security. Neither of these behaviors are mandated by the

standard, and are therefore implementation independent.

Test #4.8: CHAP_N Different Name

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:39:45 2003

Discussion: There is no requirement that the CHAP_N value cannot be reused, reflected, changed, or unchanged.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a session of SessionType=Normal to the DUT. After the first connection reaches the Full Feature Phase, the Testing Station should start a second connection.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C on each connection.
· On each connection the Testing Station should offer appropriate CHAP_N and CHAP_R responses. The DUT should offer the different CHAP_I and CHAP_C values. The Testing Station should offer different CHAP_N values on each connection.

Observable Results:
· The DUT may choose to transmit Login Reject to the unknown CHAP_N. The DUT may choose to accept the unknown CHAP_N, if it has a weak implementation of CHAP.

Possible Problems: An implementation may choose to accept only CHAP_N values it has been configured to accept. This would be a strong implementation of CHAP security. An implementation also could choose to accept any CHAP_N value. This would be a weak implementation of CHAP security. Neither of these behaviors are mandated by the standard, and are therefore implementation independent.

Test #5.1: CHAP_R Invalid Value

Purpose: To see that the DUT properly responds to a received CHAP_R key=value pair.

Reference: 8.2, RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:39:56 2003

Discussion: The CHAP_R value should be formatted as a binary and 16 bytes in length.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer appropriate CHAP_N response. The Testing Station should offer a CHAP_R, of size 16 bytes, formatted as a binary, but not the correct calculation from the given CHAP_C and CHAP Secret .

Observable Results:
· Verify that the DUT transmits Login Reject with status 'Authentication Failure'.

Possible Problems: None.

Test #5.2: CHAP_R Too Big

Purpose: To see that the DUT properly responds to a received CHAP_R key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:40:06 2003

Discussion: The CHAP_R value should be formatted as a binary and 16 bytes in length.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer appropriate CHAP_N response. The Testing Station should offer a CHAP_R, of size 20 bytes, formatted as a binary, but not the correct calculation from the given CHAP_C and CHAP Secret .

Observable Results:
· Verify that the DUT transmits Login Reject with status 'Authentication Failure'.

Possible Problems: None.

Test #5.3: CHAP_R Too Small

Purpose: To see that the DUT properly responds to a received CHAP_R key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:40:12 2003

Discussion: The CHAP_R value should be formatted as a binary and 16 bytes in length.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer appropriate CHAP_N response. The Testing Station should offer a CHAP_R, of size 14 bytes, formatted as a binary, but not the correct calculation from the given CHAP_C and CHAP Secret .

Observable Results:
· Verify that the DUT transmits Login Reject with status 'Authentication Failure'.

Possible Problems: None.

Test #5.4.1: CHAP_R Out of Order

Purpose: To see that the DUT properly responds to a received CHAP_R key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:40:20 2003

Discussion: The CHAP_R value should be formatted as a binary and 16 bytes in length.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer appropriate CHAP_N CHAP_I and CHAP_C response. The Testing Station should not offer CHAP_R.

Observable Results:
· Verify that the DUT does not respond to the received CHAP_N, I and C by sending a Login Response with CHAP_N and CHAP_R, as this would violate the step definition. The DUT can choose to send an empty Login Response, indicating that it is waiting for the Testing Station to transmit CHAP_R to complete the step.

Possible Problems: The DUT may transmit a Login Reject. Although none of the behavior described in the procedure is illegal, a Login Reject is acceptable.

Test #5.4.2: CHAP_R Out of Order

Purpose: To see that the DUT properly responds to a received CHAP_R key=value pair.

Reference: RFC 1994 4.1

Resource Requirements: A Test Generator tool capable of producing iSCSI PDUs and transporting them over a TCP connection.

Last Modification: Mon Jun 16 16:40:27 2003

Discussion: The CHAP_R value should be formatted as a binary and 16 bytes in length.

Test Setup: The DUT and Test Station pair should be able to make a TCP connection.

Procedure:
· Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
· Open a normal session to the DUT.
· On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
· The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
· The Testing Station should offer appropriate CHAP_R CHAP_I and CHAP_C response. The Testing Station should not offer CHAP_N.

Observable Results:
· Verify that the DUT does not respond to the received CHAP_R, I and C by sending a Login Response with CHAP_N and CHAP_R, as this would violate the step definition. The DUT can choose to send an empty Login Response, indicating that it is waiting for the Testing Station to transmit CHAP_N to complete the step.

Possible Problems: The DUT may transmit a Login Reject. Although none of the behavior described in the procedure is illegal, a Login Reject is acceptable.