# iSCSI CONSORTIUM

## Initiator CHAP Test Suite
***Version 0.2***

*Technical Document*


*Last Updated: 9 July 2007 7/9/07*

*© 2007 University of New Hampshire InterOperability Laboratory*

***iSCSI Consortium***
***InterOperability Laboratory***
***University of New Hampshire***

***121 Technology Drive, Suite 2***
***Durham, NH 03824***
***Phone: (603) 862-908***
***Fax: (603) 862-4181***
http://www.iol.unh.edu/consortiums/iscsi

# TABLE OF CONTENTS



*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

# MODIFICATION RECORD

1. Currently on Version 0.1, initial release.
2. Aaron Bascom: Version 0.2. Updated tests 3.6.2, 3.6.4, and 3.8.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

# 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
Aaron Bascom University of New Hampshire

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

# 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 *IETF RFC 3720 iSCSI 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.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**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.

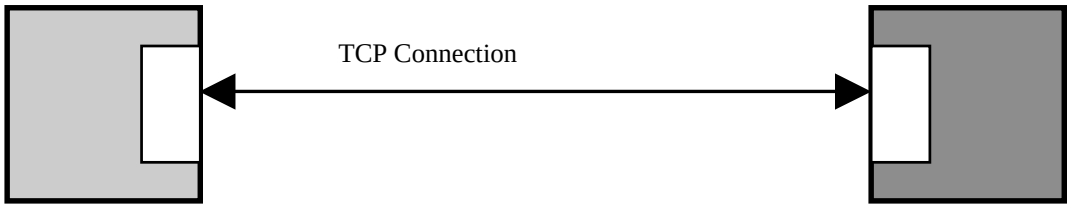
**Possible Problems**
This section provides some clues to look for if the test does not yield the expected results.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

# TEST SETUPS

The following test setups are used in this test suite:

Test Setup 1:




Testing Station/ Monitor DUT

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #1.1: CHAP_A Valid Value**

**Purpose:** To see that the DUT properly transmits and receives the 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:** Tue Jun 24 09:20:38 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer CHAP_A=5.The Testing Station should respond with CHAP_A=5 and valid values for CHAP_C and CHAP_I.

**Observable Results:**
· Verify that the DUT offers CHAP_A=5.
· Verify that upon receiving the CHAP_I and CHAP_C keys, the DUT transmits accurate values for CHAP_N and CHAP_R. CHAP_N is a string up to 255 bytes and CHAP_R is a binary 16 bytes in length.

**Possible Problems:** The DUT may require Target Authentication.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #1.2.1: CHAP_A Invalid Value**

**Purpose:** To see that the DUT properly transmits and receives the 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:** Tue Jun 24 09:20:47 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer CHAP_A=5.The Testing Station should respond with CHAP_A=7.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** None.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #1.2.2: CHAP_A Invalid Value**

**Purpose:** To see that the DUT properly transmits and receives the 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:** Tue Jun 24 09:20:58 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer CHAP_A=5.The Testing Station should respond with CHAP_A=Five.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** None.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #1.3: CHAP_A Out of Order**

**Purpose:** To see that the DUT properly responds to an out of order CHAP_A key.

**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 Jul 7 12:26:36 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP, CHAP_A=5.

**Observable Results:**
· Verify that the DUT closes the connection or transmits Login Reject with status detail of 'Initiator Error'

**Possible Problems:** None.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #2.1: CHAP_I Valid Value**

**Purpose:** To see that the DUT properly responds to an out of order CHAP_A key.

**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 Jun 24 09:21:17 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and valid values for CHAP_I and CHAP_C.

**Observable Results:**
· Verify that the DUT responds with valid values for CHAP_N and CHAP_R, and that if it chooses to request Target it offers a CHAP_C between 1 and 1024 bytes, and CHAP_I one byte in length.

**Possible Problems:** The DUT may not request Target Authentication, in which case this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #2.2: CHAP_I Invalid Value**

**Purpose:** To see that the DUT properly responds to an out of order CHAP_A key.

**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 Jun 24 09:21:26 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value CHAP_C, but CHAP_I should be 2 bytes long.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** The DUT may not request Target Authentication, in which case this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #2.3: CHAP_I Out of Order**

**Purpose:** To see that the DUT properly responds to an out of order CHAP_I key.

**Reference:** 11.1.4

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

**Last Modification:** Thu Jul 10 10:40:13 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP,None. The Testing Station is expected to respond with Authmethod=CHAP, CHAP_I=I.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** The DUT may not request Target Authentication, in which case this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #2.4: CHAP_I Same Value**

**Purpose:** To see that the DUT properly responds to receiving the same CHAP_I key-value pair on different connections.

**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 Jun 24 09:21:41 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open 2 connections to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP on each connection. The Testing Station is expected to respond with AuthMethod=CHAP on each connection.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_C different on each connection. The Testing Station should offer the same CHAP_I on each connection.

**Observable Results:**
· Verify that the DUT continues the CHAP Authentication process and does not transmit Login Reject.

**Possible Problems:** None.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #2.5: CHAP_I Reflected**

**Purpose:** To see that the DUT properly responds to receiving the same CHAP_I key-value pair on different connections.

**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 Jun 24 09:21:49 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open 2 connections to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP on each connection. The Testing Station is expected to respond with AuthMethod=CHAP on each connection.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_C different on each connection. The Testing Station should offer the same CHAP_I on on the second connection as the DUT offered while requesting Target Authentication on the first connection.

**Observable Results:**
· Verify that the DUT continues the CHAP Authentication process and does not transmit Login Reject.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #2.6: CHAP_I Different**

**Purpose:** To see that the DUT properly responds to receiving the same CHAP_I key-value pair on different connections.

**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 Jun 24 09:21:58 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open 2 connections to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP on each connection. The Testing Station is expected to respond with AuthMethod=CHAP on each connection.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_C different on each connection. The Testing Station should offer a different CHAP_I on each connection.

**Observable Results:**
· Verify that the DUT continues the CHAP Authentication process and does not transmit Login Reject.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.1: CHAP_C Big Value**

**Purpose:** To see that the DUT properly responds to receiving a large CHAP_C 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 Jun 24 09:22:51 2003

**Discussion:** The CHAP_C key is expected to be between 1 and 1024 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I. The Testing Station should offer a value for CHAP_C which is 1024 bytes in length.

**Observable Results:**
· Verify that the DUT continues the CHAP Authentication process and does not transmit Login Reject.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.2: CHAP_C Small Value**

**Purpose:** To see that the DUT properly responds to receiving a large CHAP_C 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:** Thu Apr 24 15:47:00 2003

**Discussion:** The CHAP_C key is expected to be between 1 and 1024 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I. The Testing Station should offer a value for CHAP_C which is 1 byte in length.

**Observable Results:**
· Verify that the DUT continues the CHAP Authentication process and does not transmit Login Reject.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.3: CHAP_C Too Big Value**

**Purpose:** To see that the DUT properly responds to receiving a large CHAP_C 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:** Thu Apr 24 15:48:44 2003

**Discussion:** The CHAP_C key is expected to be between 1 and 1024 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I. The Testing Station should offer a value for CHAP_C which is 1028 bytes in length.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.4: CHAP_C Too Small Value**

**Purpose:** To see that the DUT properly responds to receiving a large CHAP_C 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:** Thu Apr 24 15:49:15 2003

**Discussion:** The CHAP_C key is expected to be between 1 and 1024 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I. The Testing Station should offer a value for CHAP_C which is 4 bits in length.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.5: CHAP_C Out of Order**

**Purpose:** To see that the DUT properly responds to an out of order CHAP_C key.

**Reference:** 11.1.4

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

**Last Modification:** Thu Jul 10 10:40:42 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP, CHAP_C=C.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** The DUT may not request Target Authentication, in which case this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.6.1: CHAP_C Same Value**

**Purpose:** To see that the DUT properly sends a different Challenge every time the CHAP_C key is sent.

**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:** Thu Apr 24 16:09:14 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 DUT and the Testing Station with different CHAP secrets.
· Allow the DUT to open 2 connections to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP on each connection. The Testing Station is expected to respond with AuthMethod=CHAP on each connection.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I different on each connection. The Testing Station should offer the same CHAP_C on each connection.

**Observable Results:**
· Verify that the DUT closes each connection.

**Possible Problems:** None.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.6.2: CHAP_C Same Value**

**Purpose:** To see that the DUT properly sends a different Challenge every time the CHAP_C key is sent.

**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:** July 9, 2007

**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 DUT and the Testing Station with different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· Complete Security Negotiation and Operational Phase Negotiation. Once in Full Feature Phase operation allow the DUT to transmit a SCSI Command.
· The Testing Station should not respond to the SCSI Command, request Logout via an Asynch Message, and close the connection.
· Allow the DUT to open new a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid new value for CHAP_I and the same CHAP_C as used in the previous connection.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** None.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.6.3: CHAP_C Same Value**

**Purpose:** To see that the DUT properly sends a different Challenge every time the CHAP_C key is sent.

**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:** Thu Apr 24 16:23:38 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 DUT and the Testing Station with different CHAP secrets.
· Allow the DUT to open 2 connections to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP on each connection. The Testing Station is expected to respond with AuthMethod=CHAP on each connection.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C. The DUT is expected to respond with CHAP_N, CHAP_R on each connection.
· If the DUT is requesting Target Authentication is should offer CHAP_I and CHAP_C.

**Observable Results:**
· Verify that the DUT offers a different CHAP_C on each connection.

**Possible Problems:** If the DUT does not support Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.6.4: CHAP_C Same Value**

**Purpose:** To see that the DUT properly sends a different Challenge every time the CHAP_C key is sent.

**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:** July 9, 2007

**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 DUT and the Testing Station with different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N and CHAP_R, and if it is requesting Target Authentication CHAP_I and CHAP_C.
· Complete Security Negotiation and Operational Phase Negotiation. Once in Full Feature Phase operation allow the DUT to transmit a SCSI Command.
· The Testing Station should ignore the SCSI Command, request Logout via an Asynch Message, and close the connection.
· Allow the DUT to open new a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid new value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_R, and CHAP_N. If the DUT is requesting Target Authentication it should also offer CHAP_C and CHAP_I.

**Observable Results:**
· Verify that the DUT uses a different CHAP_C on each connection.

**Possible Problems:** If the DUT does not support Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.7: CHAP_C Reflect**

**Purpose:** To see that the DUT properly responds to an out of order CHAP_C key.

**Reference:** 11.1.4

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

**Last Modification:** Thu Apr 24 16:51:51 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. The initiator MUST continue with: CHAP_N=N CHAP_R=R or, if it requires target authentication, with: CHAP_N=N CHAP_R=R CHAP_I=I CHAP_C=C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication CHAP_C and CHAP_I.

**Observable Results:**
· Verify that the CHAP_C used by the DUT is different than the one offered by the Testing Station.

**Possible Problems:** The DUT may not request Target Authentication, in which case this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #3.8: CHAP_C Reflected**

**Purpose:** To see that the DUT properly sends a different Challenge every time the CHAP_C key is sent.

**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:** July 9, 2007

**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 DUT and the Testing Station with different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· Complete Security Negotiation and Operational Phase Negotiation. Once in Full Feature Phase operation allow the DUT to transmit a SCSI Command.
· The Testing Station should ignore the SCSI Command, request Logout via an Asynch Message, and close the connection.
· Allow the DUT to open new a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid new value for CHAP_I and the same CHAP_C as used by the DUT in the previous connection.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** None.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #4.1: CHAP_N Valid Value**

**Purpose:** To see that the DUT properly responds to receiving a valid CHAP_N and CHAP_R 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 Apr 28 15:41:03 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with appropriate CHAP_N and CHAP_R values.

**Observable Results:**
· Verify that the DUT continues the CHAP Authentication process and sets the T bit with NSG set to Operational Parameter Negotiation or Full Feature Phase operation.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #4.2: CHAP_N Big Value**

**Purpose:** To see that the DUT properly responds to receiving a valid CHAP_N 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 Apr 28 15:49:20 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_N is expected to be within 1-255 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with appropriate CHAP_N and CHAP_R values. The CHAP_N value should be 255 bytes in length.

**Observable Results:**
· Verify that the DUT continues the CHAP Authentication process and sets the T bit with NSG set to Operational Parameter Negotiation or Full Feature Phase operation.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #4.3: CHAP_N Small Value**

**Purpose:** To see that the DUT properly responds to receiving a valid CHAP_N 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 Apr 28 15:49:51 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_N is expected to be within 1-255 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with appropriate CHAP_N and CHAP_R values. The CHAP_N value should be 1 byte in length.

**Observable Results:**
· Verify that the DUT continues the CHAP Authentication process and sets the T bit with NSG set to Operational Parameter Negotiation or Full Feature Phase operation.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #4.4: CHAP_N Too Big Value**

**Purpose:** To see that the DUT properly responds to receiving an invalid CHAP_N 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:** Thu Jul 10 10:32:34 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_N is expected to be within 1-255 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with appropriate CHAP_N and CHAP_R values. The CHAP_N value should be 256 bytes in length.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #4.5: CHAP_N Out of Order**

**Purpose:** To see that the DUT properly responds receiving a valid CHAP_N key-value pair in a manner which violates the step definitions.

**Reference:** 11.1.4

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

**Last Modification:** Thu Jul 10 10:41:10 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_N is expected to be within 1-255 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP, CHAP_N.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #4.6: CHAP_N Reflected**

**Purpose:** To see that the DUT properly responds to receiving a refelcted, yet valid, CHAP_N 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:** Thu Jul 10 10:34:03 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_N is expected to be within 1-255 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station. During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with an appropriate CHAP_R value. The CHAP_N key=value pair should also be offered, and be the same value for CHAP_N that the DUT used.

**Observable Results:**
· Verify that the DUT continues with Login Phase negotiation by setting the T bit and setting NSG to Operational Negotiation or Full Feature Phase.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #4.7: CHAP_N Same**

**Purpose:** To see that the DUT properly responds to receiving a previously seen valid CHAP_N 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:** Thu Jul 10 10:34:35 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_N is expected to be within 1-255 bytes.

**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 different CHAP secrets.
· Allow the DUT to open 2 connections to the Testing Station.
·On each connection the DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· On each connection during the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· On each connection the DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· On each connection the Testing Station should reply to the received CHAP_I and CHAP_C with an appropriate CHAP_R value. The CHAP_N key=value pair should also be offered, and be the same value for CHAP_N on each connection.

**Observable Results:**
· Verify that the DUT continues with Login Phase negotiation by setting the T bit and setting NSG to Operational Negotiation or Full Feature Phase.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #4.8: CHAP_N Different**

**Purpose:** To see that the DUT properly responds to receiving a valid CHAP_N 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:** Thu Jul 10 10:34:56 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_N is expected to be within 1-255 bytes.

**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 different CHAP secrets.
· Allow the DUT to open 2 connections to the Testing Station.
·On each connection the DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· On each connection during the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· On each connection the DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· On each connection the Testing Station should reply to the received CHAP_I and CHAP_C with an appropriate CHAP_R value. The CHAP_N key=value pair should also be offered, and be a different value for CHAP_N on each connection.

**Observable Results:**
· Verify that the DUT continues with Login Phase negotiation by setting the T bit and setting NSG to Operational Negotiation or Full Feature Phase.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #5.1: CHAP_R Invalid Value**

**Purpose:** To see that the DUT properly responds to receiving an invalid CHAP_R 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 Apr 28 16:49:19 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_R is expected to be 16 bytes.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with an appropriate CHAP_N value. The CHAP_R value offered should be 16 bytes in length but not the correct response for the offered CHAP_C and configured CHAP Secret.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #5.2: CHAP_R Too Big Value**

**Purpose:** To see that the DUT properly responds to receiving an invalid CHAP_R 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 Apr 28 16:49:03 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_R is expected to be 16 bytes long.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with an appropriate CHAP_N value. The CHAP_R value offered should be 20 bytes in length.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #5.3: CHAP_R Too Small Value**

**Purpose:** To see that the DUT properly responds to receiving an invalid CHAP_R 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 Apr 28 16:50:40 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_R is expected to be 16 bytes long.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with an appropriate CHAP_N value. The CHAP_R value offered should be only the first 14 bytes of the correct CHAP_R value.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*

**Test #5.4: CHAP_R Out of Order**

**Purpose:** To see that the DUT properly responds to receiving a CHAP_R key-value pair, in a manner that violates the step definition.

**Reference:** 11.1.4

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

**Last Modification:** Thu Jul 10 10:35:37 2003

**Discussion:** An initiator requesting Target Authentication expects to receive CHAP_N and CHAP_R in response to an offered CHAP_I and CHAP_C. CHAP_R is expected to be 16 bytes long.

**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 different CHAP secrets.
· Allow the DUT to open a connection to the Testing Station.
· The DUT should attempt to perform a Security Negotiation Phase with the Testing Station.
· During the Security Negotiation Phase of Login, the DUT should offer AuthMethod=CHAP. The Testing Station is expected to respond with AuthMethod=CHAP.
· The DUT should offer valid values for CHAP_A=5, the Testing Station should reply with CHAP_A=5, and a valid value for CHAP_I and CHAP_C.
· The DUT is expected to respond with CHAP_N, CHAP_R, and if requesting Target Authentication, CHAP_I and CHAP_C.
· The Testing Station should reply to the received CHAP_I and CHAP_C with an appropriate CHAP_N value. The CHAP_R key should not be offered.

**Observable Results:**
· Verify that the DUT closes the connection.

**Possible Problems:** If the DUT does not request Target Authentication this item is not testable.

*Copyright (c) 2007 University of New Hampshire. All Rights Reserved*