iSCSI CONSORTIUM

Initiator CHAP Test Suite
Version 2.0

Technical Document

Last Updated: 9 December 2011

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

The University of New Hampshire
InterOperability Laboratory

DIGITAL SIGNATURE INFORMATION

This document was created using an Adobe digital signature. A digital signature helps to ensure the authenticity of the document, but only in this digital format. For information on how to verify this document's integrity proceed to the following site:

http://www.iol.unh.edu/certifyDoc/index.html

If the document status still indicates "Validity of author NOT confirmed", then please contact the UNH-IOL to confirm the document's authenticity. To further validate the certificate integrity, Adobe 6.0 should report the following fingerprint information:

MD5 Fingerprint: 4B9E 655C 582A 3980 84EF 7C0A BCED 1EBF
SHA-1 Fingerprint: 02CB 7B8F F1EC 5921 DE3F A21B 6606 B809 12D9 DD0E

TABLE OF CONTENTS

The University of New Hampshire
InterOperability Laboratory

MODIFICATION RECORD

[1] July 10, 2003 (Version 0.1) DRAFT RELEASE

David Woolf:	Initial draft release to draft 20 of the iSCSI standard.

[2] July 9, 2007 (Version 0.2) FINAL RELEASE

Aaron Bascom:	Test Suite updated to match final RFC 3720 standard. Updated tests 3.6.2, 3.6.4, and 3.8.

[3] August 14, 2007 (Version 1.0) FINAL RELEASE

Aaron Bascom:	Changed title page.

[4] December 8, 2011 (Version 2.0) FINAL RELEASE

Mark Niemeyer:	Test Suite updated to match RFC 5048 standard. Renamed tests 3.6.1-3.6.4 to have unique names. Tests 2.4, 3.6.1, and 3.6.2 made informative. Updated formatting.
Patrick MacArthur:	Added Additional Acronyms and Abbreviations section. Minor formatting changes. Fix typo in Purpose section of test 2.6. Updated tests 3.3, 5.2, 5.3: Test 1 above/below the limit Updated test 5.2: Ensure first 16 bytes are valid Tests 1.2.1, 1.2.2, 3.3, 3.6.1, 3.6.2, 3.6.3, 3.6.4: updated purpose statement Tests 2.4, 2.5, 2.6: Add Possible Problem for MC/S. Added tests 5.5, 5.6.

The University of New Hampshire
InterOperability Laboratory

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
Mark Niemeyer	University of New Hampshire
Patrick MacArthur	University of New Hampshire

INTRODUCTION

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 particular suite of tests has been developed to help implementers evaluate the Challenge Handshake Authentication Protocol (CHAP) functionality of their iSCSI targets.

These tests are designed to determine if an iSCSI product conforms to specifications defined in both ***IETF RFC 3720 iSCSI*** (hereafter referred to as the "iSCSI Standard") as well as updates as contained in ***IETF RFC 5048 iSCSI Corrections and Clarifications*** (hereafter referred to as "iSCSI Corrections and Clarifications"). Conformance to ***IETF RFC 1994 CHAP*** (hereafter referred to as the "CHAP Standard") is tested only when required by the iSCSI Standard or iSCSI Corrections and Clarifications. Successful completion of all tests contained in this suite does not guarantee that the tested device will successfully operate with other iSCSI products. However, when combined with satisfactory operation in the IOL's interoperability test bed, these tests provide a reasonable level of confidence that the Device Under Test (DUT) will function properly in many iSCSI environments.

The tests contained in this document are organized in order to simplify the identification of information related to a test, and to facilitate in the actual testing process. Tests are separated into groups, primarily in order to reduce setup time in the lab environment, however the different groups typically also tend to focus on specific aspects of device functionality. A dot-notated naming system is used to catalog the tests, where the first number always indicates a specific group of tests in which the test suite is based. The second and third numbers indicate the test's group number and test number within that group, respectively. This format allows for the addition of future tests in the appropriate groups without requiring the renumbering of the subsequent tests.

The test definitions themselves are intended to provide a high-level description of the motivation, resources, procedures, and methodologies specific to each test. Formally, each test description contains the following sections:

Purpose

The purpose is a brief statement outlining what the test attempts to achieve. The test is written at the functional level.

References

This section specifies all reference material *external* to the test suite, including the specific sub clauses references for the test in question, and any other references that might be helpful in understanding the test methodology and/or test results. External sources may also be referenced by a bracketed number (e.g., [1]) when mentioned in the test description. Any other references in the test description that are not indicated in this manner refer to elements within the test suite document itself (e.g., "Appendix 5.A", or "Table 5.1.1-1")

Resource Requirements

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

Last Modification

This specifies the date of the last modification to this test.

Discussion

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

Test Setup

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

Procedure

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

Observable Results

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

Possible Problems

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

REFERENCES

The following documents are referenced in this text:

CHAP Standard IETF RFC 1994
iSCSI Standard IETF RFC 3720
iSCSI Corrections and Clarifications IETF RFC 5048

ADDITIONAL ACRONYMS AND ABBREVIATIONS

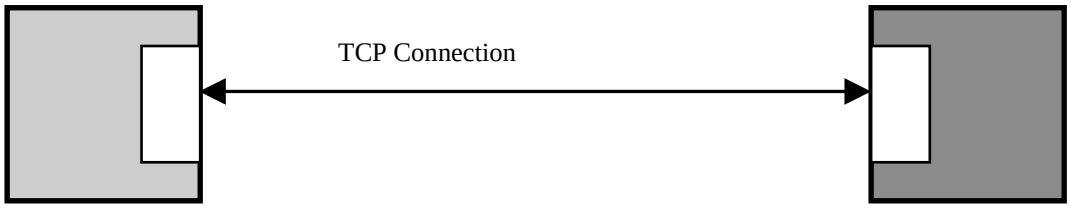
The acronyms and abbreviations defined here supplement the acronyms defined in IETF RFC 3720 section 2.2 and may be used in this document.

Acronym	Definition
DUT	Device Under Test
DDTL	DesiredDataTransferLength
DSL	DataSegmentLength
EDTL	ExpectedDataTransferLength
MRDSL	MaxRecvDataSegmentLength
READ CAP	READ CAPACITY
TMF	Task Management Function

TEST SETUPS

The following test setups are used in this test suite:

Test Setup 1:



Testing Station/ Monitor DUT

GROUP 1: CHAP_A VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_A key, defined in RFC 3720 and updated in RFC 5048. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Peter Scruton, UNH InterOperability Lab (pjs@iol.unh.edu).

Test #1.1: CHAP_A Valid Value

Purpose: To verify that the DUT properly transmits and receives the CHAP_A key=value pair.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 3

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

Last Modification: August 2, 2010

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. A value of CHAP_A = 5 is required by RFC 1994. The value 5 indicates support for CHAP with the MD5 hash algorithm. 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 value 16 bytes in length.

Possible Problems: None.

Test #1.2.1: CHAP_A Invalid Numeric Value

Purpose: To verify that the DUT properly recognizes an invalid CHAP_A key=value pair response that contains an algorithm that was not offered.

Reference: iSCSI Standard Clause 8.2, 11.1.4

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

Last Modification: October 18, 2011

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. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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.

Test #1.2.2: CHAP_A Invalid Non-Numeric Value

Purpose: To verify that the DUT properly recognizes a non-numeric CHAP_A key=value pair response.

Reference: iSCSI Standard Clause 8.2, 11.1.4

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

Last Modification: October 18, 2011

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. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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.

Test #1.3: CHAP_A Out of Order

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

Reference: iSCSI Standard Clause 8.2, 11.1, 11.1.4

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

Last Modification: August 2, 2010

Discussion: The authentication method proposal may be made by either the initiator or the target. However the initiator MUST make the first step specific to the selected authentication method as soon as it is selected. It follows that if the target makes the authentication method proposal the initiator sends the first keys(s) of the exchange together with its authentication method selection. 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. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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 Testing Station should offer AuthMethod=CHAP, CHAP_A=5.

Observable Results:

- Verify that the DUT closes the connection.

Possible Problems: None.

GROUP 2: CHAP_I VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_I key, defined in RFC 3720 and updated in RFC 5048. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Peter Scruton, UNH InterOperability Lab (pjs@iol.unh.edu).

Test #2.1: CHAP_I Valid Value

Purpose: To verify that the DUT properly responds to a valid CHAP_I key.

Reference: iSCSI Standard Clause 11.1.4

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

Last Modification: August 2, 2010

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.
- If the DUT chooses to request Target Authentication, verify that it offers a CHAP_C between 1 and 1024 bytes, and CHAP_I one byte in length.

Possible Problems: None.

Test #2.2: CHAP_I Invalid Value

Purpose: To verify that the DUT properly responds to an invalid CHAP_I value.

Reference: iSCSI Standard Clause 8.2, 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: August 2, 2010

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. Where N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994]. The Identifier field is one octet. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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: None.

Test #2.3: CHAP_I Out of Order

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

Reference: iSCSI Standard Clause 8.2, 11.1, 11.1.4

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

Last Modification: August 2, 2010

Discussion: The authentication method proposal may be made by either the initiator or the target. However the initiator MUST make the first step specific to the selected authentication method as soon as it is selected. It follows that if the target makes the authentication method proposal the initiator sends the first keys(s) of the exchange together with its authentication method selection. 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. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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_I=[Any valid value].

Observable Results:

- Verify that the DUT closes the connection.

Possible Problems: None.

Test #2.4: CHAP_I Same Value (Informative)

Purpose: To verify that the DUT properly responds to receiving the same CHAP_I key-value pair on different connections. This test is for informative purposes only.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1, iSCSI Corrections and Clarifications Clause 7.4

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

Last Modification: October 18, 2011

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. The Identifier field MUST be changed each time a Challenge is sent.

Unless [RFC3720] or [RFC5048] requires it, an iSCSI implementation is not required to do an exhaustive protocol conformance check on an incoming iSCSI PDU. The iSCSI implementation especially is not required to double-check the remote iSCSI implementation's conformance to protocol requirements.

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 terminate the connection. The DUT may also disconnect if it has a strong implementation of CHAP.

Possible Problems: Neither iSCSI document mandates that received CHAP_I values be checked for reuse. It is therefore not required for the DUT to detect the testing station’s violation of the CHAP Standard. However, a strong implementation of CHAP may perform exhaustive protocol conformance checking on the received PDU and detect the reused CHAP_I value. Therefore, it is acceptable for an implementation of CHAP to terminate the connection.

If the DUT does not support multiple connections per session or does not attempt to open 2 connections to the Testing Station, this test is Not Testable.

Test #2.5: CHAP_I Reflected

Purpose: To verify that the DUT properly responds to receiving a reflected CHAP_I key-value pair on different connections.

Reference: iSCSI Standard Clause 11.1.4

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

Last Modification: October 18, 2011

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 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 terminate the connection.

Possible Problems: If the DUT does not support multiple connections per session or does not attempt to open 2 connections to the Testing Station, this test is Not Testable.

Test #2.6: CHAP_I Different

Purpose: To verify that the DUT properly responds to receiving different CHAP_I key-value pairs on different connections.

Reference: iSCSI Standard Clause 11.1.4

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

Last Modification: October 18, 2011

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 terminate the connection.

Possible Problems: If the DUT does not support multiple connections per session or does not attempt to open 2 connections to the Testing Station, this test is Not Testable.

GROUP 3: CHAP_C VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_C (CHAP Challenge) key, defined in RFC 3720 and updated in RFC 5048. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Peter Scruton, UNH InterOperability Lab (pjs@iol.unh.edu).

Test #3.1: CHAP_C Big Value

Purpose: To verify that the DUT properly responds to receiving a large, but valid, CHAP_C value.

Reference: iSCSI Standard Clause 11.1.4

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

Last Modification: August 2, 2010

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. Where N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994], N is a text string, A,A1,A2, and I are numbers, and C and R are large-binary-values and their binary length (not the length of the character string that represents them in encoded form) MUST not exceed 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 terminate the connection.

Possible Problems: None.

Test #3.2: CHAP_C Small Value

Purpose: To verify that the DUT properly responds to receiving a small, but valid CHAP_C value.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: August 2, 2010

Discussion: N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994]. The Challenge Value is a variable stream of octets.

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 terminate the connection.

Possible Problems: None.

Test #3.3: CHAP_C Too Big Value

Purpose: To verify that the DUT properly responds to receiving an invalid CHAP_C key-value pair that has a value larger than the size allowed by the iSCSI Standard.

Reference: iSCSI Standard Clause 8.2, 11.1.4

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

Last Modification: October 18, 2010

Discussion: CHAP_C and CHAP_R are large-binary-values and their binary length (not the length of the character string that represents them in encoded form) MUST not exceed 1024 bytes. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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 1025 bytes in length.

Observable Results:

- Verify that the DUT closes the connection.

Possible Problems: None.

Test #3.4: CHAP_C Too Small Value

Purpose: To verify that the DUT properly responds to receiving an invalid CHAP_C key-value pair that has a value that is below the size required by the iSCSI Standard.

Reference: iSCSI Standard Clause 8.2, 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: August 2, 2010

Discussion: N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994]. The Challenge Value is a variable stream of octets. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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: None.

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: iSCSI Standard Clause 8.2, 11.1.4

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

Last Modification: August 2, 2010

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. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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: None.

Test #3.6.1: CHAP_C Same Value Parallel Detection (Informative)

Purpose: To verify that the DUT recognizes reused Challenge values within a session. This test is for informative purposes only.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1, iSCSI Corrections and Clarifications Clause 7.4

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

Last Modification: October 18, 2011

Discussion: The Challenge value MUST be changed each time a Challenge is sent. Unless [RFC3720] or [RFC5048] require it, an iSCSI implementation is not required to do an exhaustive protocol conformance check on an incoming iSCSI PDU. The iSCSI implementation especially is not required to double-check the remote iSCSI implementation's conformance to protocol requirements.

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:

- The DUT should close each connection if it has a strong implementation of CHAP. The DUT may also accept the reused CHAP_C.

Possible Problems: Neither iSCSI document mandates that received CHAP_C values be checked for reuse. It is therefore not required for the DUT to detect the testing station's violation of the CHAP Standard. However, a strong implementation of CHAP may perform exhaustive protocol conformance checking on the received PDU and detect the reused CHAP_C value. Therefore, it is acceptable for an implementation of CHAP to terminate each connection.

If the DUT does not support multiple connections per session or does not attempt to open 2 connections to the Testing Station, this test is Not Testable.

Test #3.6.2: CHAP_C Same Value Serial Detection (Informative)

Purpose: To verify that the DUT recognizes reused Challenge values between different sessions. This test is for informative purposes only.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1, iSCSI Corrections and Clarifications Clause 7.4

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

Last Modification: October 18, 2 011

Discussion: The Challenge value MUST be changed each time a Challenge is sent. Unless [RFC3720] or [RFC5048] require it, an iSCSI implementation is not required to do an exhaustive protocol conformance check on an incoming iSCSI PDU. The iSCSI implementation especially is not required to double-check the remote iSCSI implementation's conformance to protocol requirements.

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 Asynchronous Message, and close the connection.
- Allow the DUT to open a new 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:

- The DUT should close each connection if it has a strong implementation of CHAP. The DUT may also accept the reused CHAP_C.

Possible Problems: Neither iSCSI document mandates that received CHAP_C values be checked for reuse. It is therefore not required for the DUT to detect the testing station’s violation of the CHAP Standard. However, a strong implementation of CHAP may perform exhaustive protocol conformance checking on the received PDU and detect the reused CHAP_C value. Therefore, it is acceptable for an implementation of CHAP to terminate the connection.

Test #3.6.3: CHAP_C Same Value Parallel Offer

Purpose: To verify that the DUT properly sends a different Challenge every time the CHAP_C key is sent within a session.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: October 18, 2011

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 it 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 request Target Authentication this item is not testable. If the DUT does not support multiple connections per session or does not attempt to open 2 connections to the Testing Station, this test is Not Testable.

Test #3.6.4: CHAP_C Same Value Serial Offer

Purpose: To verify that the DUT properly sends a different Challenge every time the CHAP_C key is sent in different sessions.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: October 18, 2011

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 Asynchronous Message, and close the connection.
- Allow the DUT to open a new 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 request Target Authentication this item is not testable.

Test #3.7: CHAP_C Reflect

Purpose: To verify that the DUT does not reflect the CHAP_C key.

Reference: iSCSI Standard Clause 8.2.1, 11.1.4

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

Last Modification: August 2, 2010

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. Originators MUST NOT reuse the CHAP challenge sent by the Responder for the other direction of a bidirectional authentication.

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.

Test #3.8: CHAP_C Reflected

Purpose: To verify that the DUT properly detects a reflection of the CHAP_C key across connections.

Reference: iSCSI Standard Clause 8.2.1, iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: August 2. 2010

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 Asynchronous Message, and close the connection.
- Allow the DUT to open a new 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.

GROUP 4: CHAP_N VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_N (CHAP Name) key, defined in RFC 3720 and updated in RFC 5048. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Peter Scruton, UNH InterOperability Lab (pjs@iol.unh.edu).

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: iSCSI Standard Clause 11.1.4

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

Last Modification: August 2, 2010

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 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.

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: iSCSI Standard Clause 5.1, 11.1.4

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

Last Modification: August 2, 2010

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. Where N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994]. If not otherwise specified, the maximum length of a simple-value (not its encoded representation) is 255 bytes, not including the delimiter (comma or zero byte).

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.

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: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: August 2, 2010

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. Where N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994]. The Name field is one or more octets representing the identification of the system transmitting the packet.

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.

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: iSCSI Standard Clause 5.1, 11.1.4

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

Last Modification: August 2, 2010

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. Where N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994]. If not otherwise specified, the maximum length of a simple-value (not its encoded representation) is 255 bytes, not including the delimiter (comma or zero byte).

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.

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: iSCSI Standard Clause 11.1.4

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

Last Modification: August 2, 2010

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_N=[anything].

Observable Results:

- Verify that the DUT closes the connection.

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

Test #4.6: CHAP_N Reflected

Purpose: To see that the DUT properly responds to receiving a reflected, yet valid, CHAP_N key-value pair.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: August 2, 2010

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. There are no limitations on the content of [CHAP_N].

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.

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: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: August 2, 2010

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. There are no limitations on the content of [CHAP_N].

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.

Test #4.8: CHAP_N Different

Purpose: To see that the DUT properly responds to receiving a valid CHAP_N key-value pair.

Reference: iSCSI Standard Clause 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: August 2, 2010

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. There are no limitations on the content of [CHAP_N].

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.

GROUP 5: CHAP_R VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_R (CHAP Response) key, defined in RFC 3720 and updated in RFC 5048. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Peter Scruton, UNH InterOperability Lab (pjs@iol.unh.edu).

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: iSCSI Standard Clause 11.1.4

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

Last Modification: August 2, 2010

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. Where N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994]. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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.

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: iSCSI Standard Clause 8.2, 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: October 18, 2011

Discussion: The length of the Response Value depends upon the hash algorithm used (16 octets for MD5). Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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 17 bytes in length, the first 16 of which should be the valid response to the CHAP_C challenge.

Observable Results:

- Verify that the DUT closes the connection.

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

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: iSCSI Standard Clause 8.2, 11.1.4, CHAP Standard Clause 4.1

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

Last Modification: October 18, 2011

Discussion: The length of the Response Value depends upon the hash algorithm used (16 octets for MD5). Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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 15 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.

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: iSCSI Standard Claus 8.2, 11.1.4

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

Last Modification: August 2, 2010

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. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

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.

Test #5.5: CHAP_R Valid Value

Purpose: To see that the DUT properly responds to receiving a valid CHAP_R key-value pair.

Reference: iSCSI Standard Clause 11.1.4

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

Last Modification: December 9, 2011

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. Where N, (A,A1,A2), I, C, and R are (correspondingly) the Name, Algorithm, Identifier, Challenge, and Response as defined in [RFC1994], N is a text string, A,A1,A2, and I are numbers, and C and R are large-binary-values and their binary length (not the length of the character string that represents them in encoded form) MUST not exceed 1024 bytes. Whenever an iSCSI initiator gets a response whose keys, or their values, are not according to the step definition, it MUST abort the connection.

The Response Value is the one-way hash calculated over a stream of octets consisting of the Identifier, followed by (concatenated with) the "secret", followed by (concatenated with) the Challenge Value. The length of the Response Value depends upon the hash algorithm used (16 octets for MD5).

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 and should be the correct response for the offered CHAP_C and configured CHAP Secret.

Observable Results:

- Verify that the CHAP_R value offered by the DUT is 16 bytes in length and is the correct response for the given CHAP_I, CHAP_C, and configured secret values.
- Verify that the CHAP_C value offered by the DUT is between 1 and 1024 bytes in length.
- Verify that after the DUT receives the CHAP_N and CHAP_R values offered by the Testing Station, 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.

Test #5.6: CHAP_R Same

Purpose: To see that the DUT properly responds to receiving a CHAP_R value that is the same CHAP_R value that the DUT would have generated for the same CHAP_C value.

Reference: iSCSI Standard Clause 8.2.1

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

Last Modification: October 18, 2011

Discussion: Any CHAP secret used for initiator authentication MUST NOT be configured for authentication of any target, and any CHAP secret used for target authentication MUST NOT be configured for authentication of any initiator. If the CHAP response received by one end of an iSCSI connection is the same as the CHAP response that the receiving endpoint would have generated for the same CHAP challenge, the response MUST be treated as an authentication failure and cause the connection to close (this ensures that the same CHAP secret is not used for authentication in both directions).

Test Setup: The DUT and Test Station pair should be able to make a TCP connection. The DUT and the Test Station should be configured to use the same CHAP secret. The DUT should be configured to request target authentication.

Procedure:

- Configure the DUT and the Testing Station with the same CHAP secret.
- 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, 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 and should be the correct response for the offered CHAP_C and configured CHAP Secret.

Observable Results:

- Verify that the DUT closes the TCP connection.

Possible Problems: If the DUT does not request Target Authentication this item is not testable. If the DUT's administrative interface disallows configuring the same CHAP secret for both the DUT and the testing station, then this test is Not Testable.