UNH IOL iSCSI CONSORTIUM

CHAP Test Suite for iSCSI Targets
Version 3.1

Technical Document

Last Updated May 17, 2016

UNH-IOL iSCSI Consortium
InterOperability Laboratory
University of New Hampshire

21 Madbury Road, Suite 100
Durham, NH 03824
Phone: (603) 862-1908
Fax: (603) 862-4181
https://www.iol.unh.edu/testing/storage/iscsi

TABLE OF CONTENTS

MODIFICATION RECORD

[1] June 16, 2003 (Version 0.1) DRAFT RELEASE
David Woolf: Initial draft release to draft 20 of the iSCSI standard

[2] February 2, 2006 (Version 1.0) FINAL RELEASE
David Woolf: Test Suite updated to match final RFC 3720 standard. Changed Observable Results of tests 4.1 and 4.4. Adjusted procedure of tests 5.2 and 5.3.

[3] January 5, 2007 (Version 1.1) FINAL RELEASE
Aaron Bascom: Changed title page.

[4] March 9, 2009(Version 2.0) FINAL RELEASE
Patrick MacArthur,
Samuel Vohr: Test Suite updated to match iSCSI Corrections and Clarifications RFC.
Updated test #2.6.1.
Renumbered all tests to make room for new "Basic CHAP Tests" test group
Added tests #1.1, 1.2, and 1.3.

[5] Febrary 11, 2016 (Version 3.1) FINAL RELEASE
Aaron Morneau Updated References to RFC 7143
Added Digital Signature Information and Acronyms as found in other test suites.
Updated formatting to match other test suites.

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	UNH InterOperability Laboratory
Aaron Bascom	UNH InterOperability Laboratory
Samuel Vohr	UNH InterOperability Laboratory
Patrick MacArthur	UNH InterOperability Laboratory
Aaron Morneau	UNH InterOperability Laboratory

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 CHAP Authentication functionality of their iSCSI targets.

These tests are designed to determine if an iSCSI product conforms to specifications defined in ***IETF RFC 7143 Internet Small Computer System Interface (iSCSI) Protocol (Consolidated)*** (hereafter referred to as the "iSCSI Standard"). 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 are always referenced by a bracketed name (e.g., [RFC-7143]) 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:

[RFC-7143] Chadalapaka, M. Satran, J. Black, D. Internet Small Computer System Interface (iSCSI) Protocol (Consolidated). RFC 7143, April 2014

[RFC-1994] Simpson, W. CHAP Standard IETF RFC 1994, August 1996

ADDITIONAL ACRONYMS AND ABBREVIATIONS

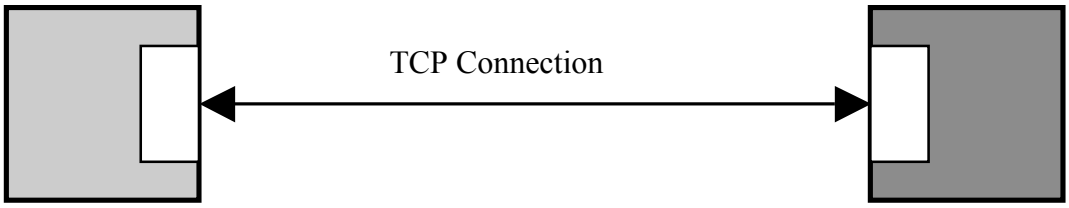
The acronyms and abbreviations defined here supplement the acronyms defined in IETF RFC 7132 section 2.1 and may be used in this document.

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: BASIC CHAP TESTS

Overview: This group of tests verifies basic CHAP functionality, defined in RFC. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Kerry Munson, UNH InterOperability Lab (kerry.munson@iol.unh.edu).

Test #1.1: Premature Transition Check

Purpose: To verify that the DUT does not transition until the initiator has been authenticated.

Reference: [RFC-7143] Section 12.1.3, 9.2

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

Last Modification: February 11, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>"

[RFC-7143] Section 9.2

> "Whenever an iSCSI target gets a response whose keys, or their values, are not according to the step definition, it MUST answer with a Login reject with the "Initiator Error" or "Missing Parameter" status."

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

Procedure:

- Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT.
- Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
- Open a normal session to the DUT.
- The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
- During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
- The Testing Station should offer CHAP_A=5. The DUT is expected to respond with CHAP_A=5 and values for CHAP_I and CHAP_C.
- The Testing Station should send an empty Login Request PDU with T=1, CSG=0, and NSG=3.

Observable Results:

- Verify that the DUT transmits a Login Response PDU with the CHAP_C=C and CHAP_I=I key=value pairs.
- Verify that the values for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a

number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.

- Verify that the DUT does not transition to Full Feature Phase, but instead sends a Login Reject PDU with status “Initiator Error” or “Missing Parameter”.

Possible Problems: There is no requirement that CHAP_A, CHAP_I, and CHAP_C be in the same Login Response PDU.

Test #1.2: Transition After Initiator Authentication

Purpose: To verify that the DUT transitions after the initiator has been authenticated.

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: February 11, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>"

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

Procedure:

- Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT.
- Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
- Open a normal session to the DUT.
- The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
- During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
- The Testing Station should offer CHAP_A=5. The DUT is expected to respond with CHAP_A=5 and values for CHAP_I and CHAP_C.
- The Testing Station should send the proper CHAP_N and CHAP_R values, with T=1, CSG=0, and NSG=1.
- Proceed through the Operational Parameter Negotiation Phase through Full Feature Phase.

Observable Results:

- Verify that the DUT transmits a Login Response PDU with the CHAP_C=C and CHAP_I=I key=value pairs.
- Verify that the values for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.

- Verify that the DUT does transition to Operational Negotiation Phase.

Possible Problems: There is no requirement that CHAP_A, CHAP_I, and CHAP_C be in the same Login Response PDU.

Test #1.3: Transition After Mutual Authentication

Purpose: To verify that the DUT transitions after the initiator and target have been authenticated.

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: February 12, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

- Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT.
- Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
- Open a normal session to the DUT.
- The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
- During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
- The Testing Station should offer CHAP_A=5. The DUT is expected to respond with CHAP_A=5 and values for CHAP_I and CHAP_C.
- The Testing Station should send the proper CHAP_N and CHAP_R values, as well as values for CHAP_I and CHAP_C to authenticate the DUT. The DUT should respond with correct values for CHAP_N and CHAP_R.
- The Testing Station should send an empty Login Request PDU with T=1, CSG=0, and NSG=1.
- Proceed through the Operational Parameter Negotiation Phase through Full Feature Phase.

Observable Results:

- Verify that the DUT transmits a Login Response PDU with the CHAP_C=C and CHAP_I=I key=value pairs.
- Verify that the values for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.
- Verify that the CHAP_N and CHAP_R values are correct.
- Verify that the DUT does transition to Operational Negotiation Phase.

Possible Problems: There is no requirement that CHAP_A, CHAP_I, and CHAP_C be in the same Login Response PDU.

GROUP 2: CHAP_A VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_A key, defined in RFC 7143. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Kerry Munson, UNH InterOperability Lab (kerry.munson@iol.unh.edu).

Test #2.1: CHAP_A Valid Value

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

Reference: [RFC-7143] Section 12.1.3, [RFC-1994] Section 3

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

Last Modification: February 12, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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."

[RFC-7143] Section 12.1.3

> "For the Algorithm, as stated in [RFC1994], one value is required to be implemented:
>
> 5 (CHAP with MD5)
>
> To guarantee interoperability, initiators MUST always offer it as one of the proposed algorithms."

[RFC-1994] Section 3

> "The Algorithm field is one octet and indicates the authentication method to be used.

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

Procedure:

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

Observable Results:

- Verify that the DUT responds the received CHAP_A key with CHAP_A=5.
- Verify that the DUT transmits a Login Response PDU with the CHAP_C=C and CHAP_I=I key=value pairs.
- Verify that the values for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a

number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.

Possible Problems: There is no requirement that CHAP_A, CHAP_I, and CHAP_C be in the same Login Response PDU.

Test #2.2: CHAP_A Valid Value In List

Purpose: To see that the DUT properly responds to a received CHAP_A key=value pair which contains a list of valid and invalid values.

Reference: [RFC-7143] Section 12.1.3, [RFC-1994] Section 3

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

Last Modification: February 11, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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."

[RFC-7143] Section 12.1.3

> "For the Algorithm, as stated in [RFC1994], one value is required to be implemented:
>
> 5 (CHAP with MD5)
>
> To guarantee interoperability, initiators MUST always offer it as one of the proposed algorithms."

[RFC-1994] Section 3

> "The Algorithm field is one octet and indicates the authentication method to be used.

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

Procedure:

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

Observable Results:

- Verify that the DUT recognizes that the required value of 5 is present
- Verify that the DUT responds the received CHAP_A key with CHAP_A=5.
- Verify that the DUT transmits a Login Response PDU with the CHAP_C=C and

CHAP_I=I key=value pairs.

- Verify that the values for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number. CHAP_C should be a binary value not exceeding 1024 bytes.

Possible Problems: There is no requirement that CHAP_A, CHAP_I, and CHAP_C be in the same Login Response PDU.

Test #2.3: CHAP_A Invalid Value

Purpose: To see that the DUT properly responds to a received CHAP_A key=value pair which does not contain a valid value.

Reference: [RFC-7143] Section 12.1.3, [RFC-1994] Section 3

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

Last Modification: January 31, 2006

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=<A> CHAP_I=<I> CHAP_C=<C> Where A is one of A1,A2... that were proposed by the initiator."

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

Procedure:

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

- Verify that the DUT recognizes that the required value of 5 is not present, and no other valid value is present. The DUT is expected to transmit a Login Reject with 'Authentication failure' as the Status code.

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

Test #2.4: CHAP_A Valid Value Not In List

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

Reference: [RFC-7143] Section 12.1.3; [RFC-1994] Section 3

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

Last Modification: January 31, 2006

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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."

[RFC-7143] Section 12.1.3

> "For the Algorithm, as stated in [RFC1994], one value is required to be implemented:
>
> 5 (CHAP with MD5)
>
> To guarantee interoperability, initiators MUST always offer it as one of the proposed algorithms."

[RFC-1994] Section 3

> "The Algorithm field is one octet and indicates the authentication method to be used.

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

Procedure:

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

Observable Results:

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

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or

'Missing Parameter'. This is acceptable.

Test #2.5: CHAP_A Present and Out of Order

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: February 11, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=<A> CHAP_I=<I> CHAP_C=<C> Where A is one of A1,A2... that were proposed by the initiator."

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

Procedure:

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

Observable Results:

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

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

Test #2.6: CHAP_A Not Received

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: February 11, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], the initiator MUST use: CHAP_A=A1 A2 Where A1,A2... are proposed algorithms, in order of preference. The target MUST answer with a Login reject with the "Authentication Failure" status or reply with: CHAP_A=<A> CHAP_I=<I> CHAP_C=<C> Where A is one of A1,A2... that were proposed by the initiator."

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

Procedure:

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

Observable Results:

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

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

GROUP 3: CHAP_I VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_I key, defined in RFC 7143. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Kerry Munson, UNH InterOperability Lab (kerry.munson@iol.unh.edu).

Test #3.1: CHAP_I Valid Value

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

Reference: [RFC -7143] Clause 12.1.3, [RFC-1994] Section 4

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

Last Modification: April 15, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-1994] Section 4

> "The Identifier field is one octet and aids in matching challenges, responses and replies."

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

Procedure:

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

Observable Results:

- Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.
- Verify that the DUT responds to the received CHAP_I and CHAP_C with a correct

CHAP_R, and also offers a valid CHAP_N. CHAP_N should be a text string between 1 and 255 bytes in length. CHAP_R should be a binary value of 16 bytes, if using MD5 hash algorithm.

Possible Problems: None.

Test #3.2: CHAP_I Invalid Value

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

Reference: [RFC -7143] Clause 12.1.3, [RFC-1994] Section 4

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

Last Modification: April 15, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-1994] Section 4

> "The Identifier field is one octet and aids in matching challenges, responses and replies."

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

Procedure:

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

Observable Results:

- Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.
- Verify that the DUT responds to the received CHAP_I with Login Reject 'Authentication

Failure' status.

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

Test #3.3: CHAP_I No Value

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

Reference: [RFC -7143] Clause 12.1.3, [RFC-1994] Section 4

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

Last Modification: April 15, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-1994] Section 4

> "The Identifier field is one octet and aids in matching challenges, responses and replies."

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

Procedure:

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

Observable Results:

- Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.

- Verify that the DUT responds to the received CHAP_I key with Login Reject 'Authentication Failure' status.

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

Test #3.4: CHAP_I Too Big Value

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

Reference: [RFC -7143] Clause 12.1.3, [RFC-1994] Section 4

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

Last Modification: April 15, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-1994] Section 4

> "The Identifier field is one octet and aids in matching challenges, responses and replies."

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

Procedure:

- Configure the Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
- Open a normal session to the DUT.
- The Testing Station should attempt to perform a Security Negotiation Phase with the DUT.
- During the Security Negotiation Phase of Login, the Testing Station should offer AuthMethod=CHAP. The DUT is expected to respond with AuthMethod=CHAP.
- The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
- The Testing Station should offer CHAP_N, CHAP_R, CHAP_I which has a value that is 2 bytes long instead of 1, and CHAP_C (8 bytes) to request Target Authentication.

Observable Results:

- Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.
- Verify that the DUT responds to the received CHAP_I key with Login Reject

'Authentication Failure' status.

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

Test #3.5.1: CHAP_I Out of Order

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

Reference: [RFC -7143] Clause 12.1.3

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

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

Observable Results:

- Verify that the DUT responds to the received CHAP_I key with Login Reject 'Authentication Failure' status.

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

Test #3.5.2: CHAP_I Out of Order

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

Reference: [RFC -7143] Clause 12.1.3

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

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

Observable Results:

- Verify that the values transmitted by the DUT for the CHAP_C and CHAP_I keys are valid. CHAP_I should be a number, no larger than 1 byte. CHAP_C should be a binary value not exceeding 1024 bytes.
- Verify that the DUT does not respond to the received CHAP_I and CHAP_C values by sending CHAP_N and CHAP_R, as this would violate the step definition. The DUT can choose to send an empty Login Response, indicating that it is waiting for the Testing

Station to transmit CHAP_N and CHAP_R to complete the step.

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

Test #3.6.1: CHAP_I Reused on Second Connection (Informative)

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair when the CHAP_I value is used on 2 connections. This test is informative only.

Reference: [RFC-7143] Section 12.1.3, 7.10, [RFC-1994] Section 4.1

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

Last Modification: April 15, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-7143] Section 7.10

"… an iSCSI implementation is not required to do an exhaustive protocol conformance check on an incoming iSCSI PDU. The iSCSI implementation in particular is not required to double-check the remote iSCSI implementation's conformance to protocol requirements.

[RFC-1994] Section 4.1

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

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

Procedure:

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

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

Observable Results:

- The DUT should reject the second instance of CHAP_I received from the Testing Station if it has a strong implementation of CHAP. The DUT may also accept the reused CHAP_I.

Possible Problems: The standard does not mandate that the target reject a reused CHAP_I. The CHAP_I value is not used directly by iSCSI, since the iSCSI protocol provides strict step definitions in order to match challenges with responses. Also, since CHAP_I is only one byte, the values will eventually be reused. Thus, an implementation of CHAP may accept a reused CHAP_I. However, although the CHAP_I value is not used directly by iSCSI, it may be used if the CHAP authentication is offloaded to another server. In addition, a reused CHAP_I value could indicate a potential replay attack. Thus, an implementation of CHAP may reject a reused CHAP_I.

Test #3.6.2: CHAP_I Different on Second Connection

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair when a second CHAP_I is used on a second connection.

Reference: [RFC-7143] Section 12.1.3, 7.10, [RFC-1994] Section 4.1

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

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

Observable Results:

- Verify that the DUT accepts each instance of CHAP_I received from the Testing Station and does not transmit Login Reject.

Possible Problems: None.

Test #3.7.1: CHAP_I Reflected

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair even when the received CHAP_I value is the same as the CHAP_I sourced by the DUT.

Reference: [RFC-7143] Section 12.1.3, 7.10, [RFC-1994] Section 4.1

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

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

Observable Results:

- Verify that the DUT accepts each instance of CHAP_I received from the Testing Station and does not transmit Login Reject.

Possible Problems: None.

Test #3.7.2: CHAP_I Reflected on Second Connection

Purpose: To see that the DUT properly responds to a received CHAP_I key=value pair even when the received CHAP_I value is the same as the CHAP_I sourced by the DUT.

Reference: [RFC-7143] Section 12.1.3, 7.10

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

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

connection and a new CHAP_C (8 bytes) to request Target Authentication.

Observable Results:

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

Possible Problems: None.

GROUP 4: CHAP_C VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_C (CHAP Challenge) key, defined in RFC 7143. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Kerry Munson, UNH InterOperability Lab (kerry.munson@iol.unh.edu).

Test #4.1: CHAP_C Reused

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

Reference: [RFC-7143] Section 12.1.3, [RFC-1994] Section 4.1

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

Last Modification: April 15, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-1994]

> "The Challenge Value MUST be changed each time a Challenge is sent."

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

Procedure:

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

Observable Results:

- Verify that the DUT uses different values for CHAP_C on each connection.

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

Test #4.2: CHAP_C Big Value

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-7143] Section 12.1.3

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

Observable Results:

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

Possible Problems: None.

Test #4.3: CHAP_C Small Value

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 15, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-1994]

> "The Value field is one or more octects."

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

Procedure:

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

Observable Results:

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

Possible Problems: None.

Test #4.4: CHAP_C Too Big Value

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

[RFC-7143] Section 12.1.3

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

Observable Results:

- Verify that the DUT end the negotiation with a Login Reject with status 'Authentication Failure'.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or

'Missing Parameter'. This is acceptable.

Test #4.5: CHAP_C Out of Order

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>. If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

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

Observable Results:

- Verify that the DUT end the negotiation with a Login Reject with status 'Authentication Failure'.

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

Test #4.6: CHAP_C Receive Reused

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

Reference: [RFC-7143] Section 9.2.1, [RFC-1994] Section 4.1

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

Last Modification: April 15, 2016

Discussion:
[RFC-7143] Section 9.2.1

> "Originators MUST NOT reuse the CHAP challenge sent by the responder for the other direction of a bidirectional authentication. Responders MUST check for this condition and close the iSCSI TCP connection if it occurs."

[RFC-1994] Section 4.1

> "The Challenge Value MUST be changed each time a Challenge is sent."

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

Procedure:

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

Observable Results:

- Verify that the DUT transmits Login Reject with 'Authentication Failure' Status. The DUT is expected to close the connection.

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

Test #4.7: CHAP_C Reflected

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

Reference: [RFC-1994] Section 4.1

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

Last Modification: April 15, 2016

Discussion:
[RFC-1994] Section 4.1

> "The Challenge Value MUST be changed each time a Challenge is sent. Originators MUST NOT reuse the CHAP challenge sent by the Responder for the other direction of a bidirectional authentication. Responders MUST check for this condition and close the iSCSI TCP connection if it occurs."

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

Procedure:

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

Observable Results:

- Verify that the DUT transmits Login Reject with 'Authentication Failure' Status.

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

Test #4.8: CHAP_C Reflected on Second Connection

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

Reference: [RFC-1994] Section 4.1

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

Last Modification: February 11, 2016

Discussion:
[RFC-1994] Section 4.1

> "The Challenge Value MUST be changed each time a Challenge is sent. Originators MUST NOT reuse the CHAP challenge sent by the Responder for the other direction of a bidirectional authentication. Responders MUST check for this condition and close the iSCSI TCP connection if it occurs."

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

Procedure:

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

Observable Results:

- Verify that the DUT transmits Login Reject with status 'Authentication Failure'.

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

Test #4.9: CHAP_C New on Second Connection

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

Reference: [RFC-1994] Section 4.1

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

Last Modification: February 11, 2016

Discussion:
[RFC-1994]

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

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

Procedure:

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

Observable Results:

- Verify that the DUT transmits valid CHAP_N and CHAP_R responses and moves on to Operational Stage Negotiation.

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

GROUP 5: CHAP_N VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_N (CHAP Name) key, defined in RFC 7143. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Kerry Munson, UNH InterOperability Lab (kerry.munson@iol.unh.edu).

Test #5.1: CHAP_N Invalid

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair where the value is not formatted as a string.

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: February 11, 2016

Discussion:
[RFC-7143] Section 12.1.3
"N is a text string"

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

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

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

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable. The DUT may require that the CHAP_N key be configured before Authentication is attempted. In this case, and the DUT will accept a configuration with CHAP_N > 255 bytes, this item is not testable. It is suggested that the interface which a user will configure CHAP_N through does not allow such an invalid configuration, but this is outside the scope of the iSCSI standard.

Test #5.2: CHAP_N Big

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

Reference: [RFC-7143] Section 6.1, 12.1.3

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

Last Modification: April 25, 2016

Discussion:
[RFC-7143] Section 6.1

> "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)."

[RFC-7143] Section 12.1.3

> "N is a text string"

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

Procedure:

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

Observable Results:

- Verify that the DUT transmits valid CHAP_N and CHAP_R in response, and does not transmit Login Reject.

Possible Problems: None.

Test #5.3: CHAP_N Small

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

Reference: [RFC-7143] Section 12.1.3, [RFC-1994] Section 4.1

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

Last Modification: April 25, 2016

Discussion:
[RFC-7143] Section 12.1.3
> "N is a text string"

[RFC-1994] Section 4.1
> "The Name field is one or more octets representing the identification of the system transmitting the packet. There are no limitations of the content of this field."

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

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

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

Possible Problems: None.

Test #5.4: CHAP_N Too Big

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

Reference: [RFC-7143] Section 6.1, 12.1.3

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

Last Modification: April 25, 2016

Discussion:
[RFC-7143] Section 6.1

> "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)."

[RFC-7143] Section 12.1.3

> "N is a text string"

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

Procedure:

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

Observable Results:

- Verify that the DUT transmits Login Reject with status of 'Authentication Failure'.

Possible Problems: The DUT may transmit a Login Reject with status of 'Initiator Error' or 'Missing Parameter'. This is acceptable. The DUT may require that the CHAP_N key be configured before Authentication is attempted. In this case, if the DUT will accept a configuration with CHAP_N > 255 bytes, this item is not testable. It is suggested that the interface which a user will configure CHAP_N through does not allow such an invalid configuration, but this is outside the scope of the iSCSI standard.

Test #5.5: CHAP_N Out of Order

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 25, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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 Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT. Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
- Open a normal session to the DUT.
- On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
- The Testing Station should offer CHAP_A=5 and CHAP_N where N is a valid value.

Observable Results:

- Verify that the DUT transmits Login Reject with status of 'Authentication Failure'.

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

Test #5.6: CHAP_N Identical

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

Reference: [RFC-7143] Section 12.1.3, [RFC-1994] Section 4.1

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

Last Modification: January 31, 2006

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>."

[RFC-1994] Section 4.1

> "The Name field is one or more octets representing the identification of the system transmitting the packet. There are no limitations of the content of this field."

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

Procedure:

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

Observable Results:

- Verify that the DUT transmits valid CHAP_N and CHAP_R in response, and does not transmit Login Reject.

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

Test #5.7: CHAP_N Reflect (Informative)

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair. This test is informative only.

Reference: [RFC-7143] Section 12.1.3, [RFC-1994] Section 4.1

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

Last Modification: January 31, 2006

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>."

[RFC-1994] Section 4.1

> "The Name field is one or more octets representing the identification of the system transmitting the packet. There are no limitations of the content of this field."

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

Procedure:

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

Observable Results:

- The DUT may choose to transmit Login Reject to the reflected CHAP_N. The DUT may choose to accept the reflected CHAP_N if it has a weak implementation of CHAP.

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

Test #5.8: CHAP_N Different Name (Informative)

Purpose: To see that the DUT properly responds to a received CHAP_N key=value pair. This test is informative only.

Reference: [RFC-7143] Section 12.1.3, [RFC-1994] Section 4.1

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

Last Modification: April 25, 2016

Discussion:

[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>."

[RFC-1994] Section 4.1

> "The Name field is one or more octets representing the identification of the system transmitting the packet. There are no limitations of the content of this field."

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

Procedure:

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

Observable Results:

- The DUT may choose to transmit Login Reject to the unknown CHAP_N. The DUT may choose to accept the unknown CHAP_N if it has a weak implementation of CHAP.

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

GROUP 6: CHAP_R VERIFICATION

Overview: This group of tests verifies the proper use of the CHAP_R (CHAP Response) key, defined in RFC 7143. Comments and questions regarding the implementation of these tests are welcome, and may be forwarded to Kerry Munson, UNH InterOperability Lab (kerry.munson@iol.unh.edu).

Test #6.1: CHAP_R Invalid Value

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

Reference: [RFC-1994] Section 4.1

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

Last Modification: April 25, 2016

Discussion:
[RFC-1994] Section 4.1

> "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."

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

Procedure:

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

Observable Results:

- Verify that the DUT transmits Login Reject with status 'Authentication Failure'.

Possible Problems: None.

Test #6.2: CHAP_R Too Big

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 25, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "R [is a binary-value]. [Its] binary length (not the length of the character string that represents [it] 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 Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT.
- Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
- Open a normal session to the DUT.
- On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
- The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
- The Testing Station should offer appropriate CHAP_N response. The Testing Station should offer a CHAP_R, of size 20 bytes, formatted as a binary, with the leading values forming the correct calculation from the given CHAP_C and CHAP Secret followed by 0's to 1024 bytes.

Observable Results:

- Verify that the DUT transmits Login Reject with status 'Authentication Failure'.

Possible Problems: None.

Test #6.3: CHAP_R Too Small

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

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 25, 2016

Discussion:
[RFC-1994] Section 4.1

> "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 Testing Station with the appropriate CHAP secret for Initiator Authentication by the DUT.
- Configure the DUT with the appropriate CHAP secret required for Target Authentication by the Testing Station.
- Open a normal session to the DUT.
- On each connection the Testing Station should attempt to perform a Security Negotiation Phase with the DUT with AuthMethod=CHAP.
- The Testing Station should offer CHAP_A=5. The DUT is expected to respond with, CHAP_A, CHAP_I, CHAP_C.
- The Testing Station should offer appropriate CHAP_N response. The Testing Station should offer a CHAP_R, of size 14 bytes, formatted as a binary, with the leading values forming the correct calculation from the given CHAP_C and CHAP Secret .

Observable Results:

- Verify that the DUT transmits Login Reject with status 'Authentication Failure'.

Possible Problems: None.

Test #6.4.1: CHAP_R Out of Order

Purpose: To see that the DUT properly responds to a received CHAP_R key=value pair when the pair is sent out of order.

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 25. 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>… If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

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

Observable Results:

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

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

Test #6.4.2: CHAP_R Out of Order

Purpose: To see that the DUT properly responds to a received CHAP_R key=value pair when the pair is transmitted out of order.

Reference: [RFC-7143] Section 12.1.3

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

Last Modification: April 25, 2016

Discussion:
[RFC-7143] Section 12.1.3

> "For CHAP [RFC1994], 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>… If the initiator authentication fails, the target MUST answer with a Login reject with "Authentication Failure" or reply with: CHAP_N=<N> CHAP_R=<R>"

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

Procedure:

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

Observable Results:

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

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