Bridge Functions Consortium

Port-Based Network Access Control
802.1X Interoperability Test Suite

Technical Document

Revision 2.0

University of New Hampshire
InterOperability Laboratory
Bridge Functions Consortium
http://www.iol.unh.edu

121 Technology Drive, Suite 2
Durham, NH 03824-4716
Phone: +1-603-862-3525
Fax: +1-603-862-4181

TABLE OF CONTENTS

MODIFICATION RECORD

Version 0.1 Complete	March 31st 2003 • Initial design [PBS for iLabs]
Version 0.2 Complete	July 16th 2004 • Initial test designs
Version 0.8 Complete	September 28th 2004 • Initial 802.1X Interoperability Draft
Version 0.85 Complete	September 30th 2004 • Review and revision
Version 0.9 Complete	October 27th 2004 • Review and revision
Version 1.0 Complete	August 8th 2005 • Review and revision
Version 1.1 Complete	September 22nd 2005 • Review and revision
Version 1.2 Complete	September 6th 2006 • Review and revision
Version 2.0 Complete	May 20th 2010 • Redid formatting • Deprecated MD5 Tests

ACKNOWLEDGEMENTS

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

Rob Bergin	The Timberland Co.
David Bond	UNH InterOperability Laboratory
Gerard Goubert	UNH InterOperability Laboratory
Deepak Jadhav	UNH InterOperability Laboratory
Fred Mansfield Jr.	UNH InterOperability Laboratory
Tyler Marcotte	UNH InterOperability Laboratory
Curtis Simonson	UNH InterOperability Laboratory
Larry B. Upson	UNH InterOperability Laboratory

INTRODUCTION

The University of New Hampshire's InterOperability Laboratory (UNH-IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard. This suite of tests has been developed to help implementers evaluate the functionality of their Port-Based Network Access Control capable products.

IEEE Std 802.1X™-2004 states:

> *"Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails. A port in this context is a single point of attachment to the LAN infrastructure."*[1]
>
> *"The mechanisms defined [in IEEE Std 802.1X™-2004] can be applied to allow any System to authenticate another System that is connected to one of its controlled Ports. The Systems concerned include end stations, servers, routers, and MAC Bridges."*[2]
>
> *"The operation of the authentication process makes use of the Extensible Authentication Protocol (EAP, specified in IETF RFC 2284) as the means of communicating authentication information between the Supplicant and the Authentication Server. EAP is a general protocol that supports multiple authentication mechanisms."*[2]

This test suite has been designed based on the set of definitions, principles, requirements and terminology that pertain to IEEE Std 802.1X™-2004. The test suite is designed to help determine whether or not the DUT will behave in accordance with the standard during normal operation.

These tests are not designed as performance tests. The relative performance of IEEE Std 802.1X™-2004 capable devices (e.g. security strength, speed of credential exchange, length of time from link to authentication of Controlled Port, etc.) is beyond the scope of this document.

These tests do not determine whether the DUT conforms to IEEE Std 802.1X™-2004, nor are they designed as conformance tests. Rather, they provide one method to isolate problems within an IEEE Std 802.1X™-2004 capable device that will affect interoperability. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other IEEE Std 802.1X™-2004 capable devices. However, combined with satisfactory completion of interoperability testing, these tests provide a reasonable level of confidence that the DUT will function well in most IEEE Std 802.1X™-2004 capable environments.

Please note that these tests are interoperability tests. Therefore, failure against a device(s) does not necessarily indicate nonconformance. Rather, it indicates that the two devices are unable to work together properly. Further work should be done to isolate the cause of the failure.

****Throughout this test suite the DUT is assumed to be an Authenticator. This test suite can be used to test interoperability of Supplicant or Authentication Server network devices.****

[1] IEEE Std 802.1X-2004: sub-clause 1.1
[2] IEEE Std 802.1X-2004: sub-clause 6.1
[2] IEEE Std 802.1X-2004: sub-clause 8.1.1

REFERENCES

The following documents are referenced in this text:

[IEEE Std 802.1X™-2004]	IEEE Computer Society LAN/MAN Standards Committee, "Port-Based Network Access Control"
[IEEE Std 802.1D™-2004]	IEEE Computer Society LAN/MAN Standards Committee, "Media Access Control (MAC) Bridges"
[IEEE Std 802.1Q™-2003]	IEEE Computer Society LAN/MAN Standards Committee, "Virtual Bridged Local Area Networks"
[RFC-1321]	Rivest, "The MD5 Message-Digest Algorithm"
[RFC-2284]	Blunk & Vollbrecht, "PPP Extensible Authentication Protocol (EAP)"
[RFC-2716]	Aboba & Simon, "PPP EAP TLS Authentication Protocol"
[RFC-2865]	Rigney, et al., "Remote Authentication Dial In User Service (RADIUS)"
[draft-josefsson-pppext-eap-tls-eap-08]	Palekar et al., "Protected EAP Protocol (PEAP) Version 2"
[draft-ietf-pppext-eap-ttls-05]	Paul Funk, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"

DEFINITION OF TERMS

Abbreviations and Acronyms:

802.1X	IEEE Std 802.1X™-2004
DUT	Device Under Test
EAP	Extensible Authentication Protocol
EAPOL	EAP over LANs
LAN	Local Area Network
PAE	Port Access Entity
PEAP	Protected EAP
Port	Network Access Port
RADIUS	Remote Authentication Dial In User Service
TLS	Transport Layer Security
TS	Test Station
TTLS	Tunneled Transport Layer Security
VLAN	Virtual Local Area Network

Definitions:

Authenticator	An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.
Authentication Server	An entity that provides an authentication service to an Authenticator, which determines, from the Supplicant's credentials, whether the Supplicant is authorized to access the services provided by the Authenticator.
Controlled Port	A point of access to the LAN that allows the exchange of PDUs only if the current state of the Port is Authorized.
DUT	An 802.1X capable MAC Bridge assuming the role of Authenticator.
EAPOL	Encapsulation techniques used to carry EAP packets between Supplicant PAEs and Authenticator PAEs in a LAN environment.
Network Access Port	A point of attachment of a system to a LAN. It can be a physical port; for example, a single LAN MAC attached to a physical LAN segment, or a logical port, for example, an IEEE 802.11 association between a station and an access point.
Network Initialization	Supplicant: initialization of EAP software on supplicant. Authenticator: initialization of Bridge entity. Authentication Server: initialization of RADIUS software on server.
Port Access Entity	The protocol entity associated with a Port. It can support the protocol functionality associated with the authenticator, the supplicant, or both.
Service	A resource offered by a System (i.e. DHCP, FTP, HTTPS, etc.)
Supplicant	An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link. Generally considered to be an end station with user access control.
System	A device that is attached to a LAN by one or more ports. Examples of systems include end stations, servers, MAC Bridges, and routers.
Uncontrolled Port	A point of access to the LAN that allows the uncontrolled exchange of PDUs between the System and other Systems on the LAN, regardless of the authorization state.

TEST ORGANIZATION

This document organizes tests by group based on related test methodology or goals. Each group begins with a brief set of comments pertaining to all tests within that group. This is followed by a series of description blocks; each block describes a single test. The format of the description block is as follows:

Test Label: The test label and title comprise the first line of the test block. The test label is the concatenation of the short test suite name, group number, and the test number within the group, separated by periods. The test number is the group number and the test number, also separated by a period. So, test label 802.1X.io.1.2 refers to the second test of the first test group in the 802.1X Interoperability suite. The test number is 1.2.

Purpose: The Purpose is a short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the feature or capability to be tested.

References: The References section lists cross-references to the specifications and documentation that might be helpful in understanding and evaluating the test and results.

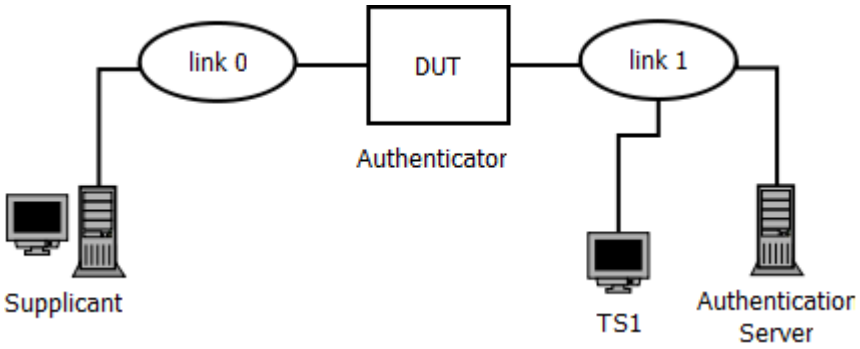
Discussion: The Discussion is a general discussion of the test and relevant section of the specification, including any assumptions made in the design or implementation of the test as well as known limitations.

Procedure: This section of the test description contains the step-by-step instructions for carrying out the test. These steps include such things as enabling interfaces, disconnecting links between devices, and sending MAC frames from a Test Station. The test procedure also cues the tester to make observations, which are interpreted in accordance with the observable results given for that test part.

Observable Results: This section lists observable results that can be examined by the tester to verify that the DUT is operating properly. When multiple observable results are possible, this section provides a short discussion on how to interpret them. The determination of a PASS or FAIL for each test is usually based on how the behavior of the DUT compares to the results described in this section.

Possible Problems: This section contains a description of known issues with the test procedure, which may affect test results in certain situations.

TEST SETUP



General 802.1X Test Setup

Note: The above diagram shows the general test setup for basic 802.1X Interoperability. For more advanced tests, a more complicated test setup may be used where appropriate.

Test System Configuration:

Each test in this suite uses the following setup for the DUT:

- If GMRP is supported, disable it.
- If GVRP is supported, disable it.
- If Spanning Tree is supported, disable it.
- Enable 802.1X on the DUT.
- Enable 802.1X on the Port on the DUT connected to the Supplicant.
- Ensure DUT is configured to utilize the correct IP address of the Authentication Server to authenticate the Supplicant's credentials.

Each test in this suite uses the following setup for a Supplicant:

- Ensure that client authentication software is installed.
- Configure authentication client to use correct authentication scheme for each test.

Each test in this suite uses the following setup for the Authentication Server:

- Ensure that the Authentication Server is configured to recognize the DUT as an authorized Authenticator.
- Ensure that a specific account on the Authentication Server for each Supplicant is configured, using the proper authentication method for each test.

Deprecated Tests

Certain tests in this test suite refer to the MD5 authentication method. MD5 has been shown to be an insecure authentication method and should therefore be avoided. These tests have been deprecated and should only be used if the device supports MD5.

GROUP 1: 802.1X Network Initialization – Unauthorized

Scope

The following tests cover the initialization of 802.1X capable devices.

Overview

The tests in this group verify that all the components of the 802.1X capable LAN function properly upon initialization and before authentication. These tests ensure that the Controlled Ports are properly restricted upon network initialization.

802.1X.io.1.1: Basic Network Initialization – Unauthorized

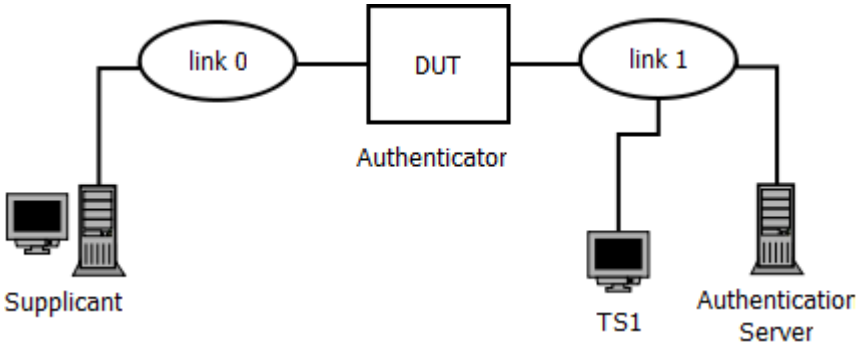
Purpose: To verify that the DUT, assuming the Authenticator role, properly restricts access to the Controlled Port before attempting to authenticate the credentials of the Supplicant.

References:

- IEEE Std 802.1X-2004

Discussion:

This test verifies that, upon network initialization and before authentication, the DUT properly places the Controlled Port, of the Port on the DUT connected to the Supplicant, in the *unauthorized* state. This action will restrict the Supplicant from accessing services offered by the LAN connected to the DUT. To verify proper restriction of the Controlled Port, the Supplicant will attempt to access services offered by the LAN connected to the DUT.



Procedure:

Part A: Basic Initialization

1. Ensure that the default test layout is connected and configured properly.
2. Do *not* enter credentials or initialize the Supplicant software.
3. Attempt to access services located on the LAN connected to the DUT.

Part B: Basic Initialization of Authenticator

4. Ensure that the default test layout is connected and configured properly.
5. Do *not* enter credentials or initialize the Supplicant software.
6. Reboot the DUT.
7. Immediately, attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In Part A, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.
- In Part B, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.

Possible Problems:

- None.

GROUP 2: Basic 802.1X Interoperability

Scope

The following tests are designed to verify the interoperability of 802.1X capable devices.

Overview

The tests in this group verify that all the components of the 802.1X capable LAN are interoperating properly. To verify this, the Supplicant uses a variety of authentication methods to authenticate via the Authenticator (DUT). Upon acceptance of authentication, the Controlled Port, of the Port on the DUT connected to the Supplicant, is placed in the *authorized* state, thereby allowing the Supplicant to gain access to services offered by the LAN connected to the DUT.

Note: If the DUT fails part A of any of the tests in this group, the proceeding parts of that test shall not be completed since the DUT will have failed basic interoperability.

802.1X.io.2.1: Basic Interoperability – MD-5 Challenge (EAP-MD5)

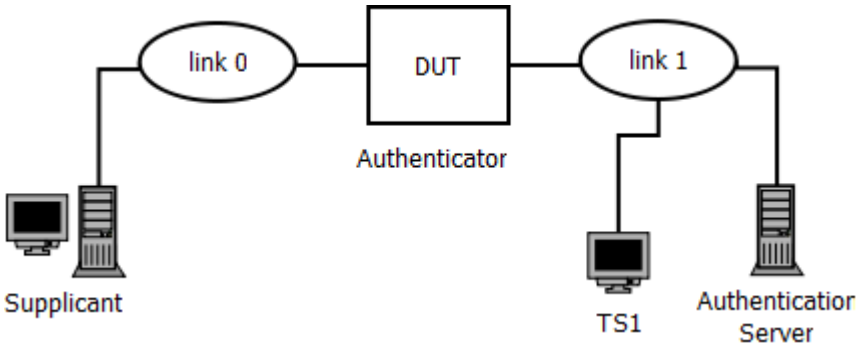
Purpose: To verify that the DUT, assuming the Authenticator role, can properly authenticate the credentials of a variety of Supplicants, using the MD-5 authentication method.

References:

- IEEE Std 802.1X-2004
  - Sub-clause 5.1 – Static conformance requirements
  - Sub-clause 6.6.4 – Logoff mechanisms
  - Sub-clause 8.2.8 – Reauthentication Timer state machine
- RFC-1321 – MD5
- RFC-2284 – EAP
- RFC-2865 – RADIUS

Discussion:

This test verifies that the DUT can properly authenticate the Supplicant's credentials, thereby allowing the Supplicant access to services offered by the LAN to which the DUT is attached. The Supplicant's credentials are authenticated by the Authentication Server via the DUT. Once the DUT has received an authentication accept message, from the Authentication Server, the Controlled Port, of the Port on the DUT connected to the Supplicant, is placed in the *authorized* state. This test has been deprecated.



Procedure:

Part A: Basic Interoperability

1. Ensure that the default test layout is connected and configured properly.
2. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
3. Attempt to access services located on the LAN connected to the DUT.

Part B: Aging out of the authorization state (set reAuthPeriod equal to 300)

4. Ensure that the default test layout is connected and configured properly.
5. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
6. Configure the *reAuthPeriod* parameter on the DUT equal to a value of 300 seconds.
7. Wait more than 300 seconds (5 minutes).
8. Attempt to access services located on the LAN connected to the DUT.

Part C: Link loss between Supplicant and Authenticator

9. Ensure that the default test layout is connected and configured properly.
10. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
11. Disconnect/reconnect the link between the Supplicant and the DUT.
12. Attempt to access services located on the LAN connected to the DUT.

Part D: Authenticator Re-initialization

13. Ensure that the default test layout is connected and configured properly.
14. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.

15. Reboot the DUT (Authenticator).
16. Allow time for the DUT to initialize and for the Supplicant to become authenticated by the Authentication Server via the DUT.
17. Attempt to access services located on the LAN connected to the DUT.

Part E: Reauthentication while in authenticated state (set reAuthEnabled equal to TRUE)

18. Ensure that the default test layout is connected and configured properly.
19. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
20. Use DUT to initiate reauthentication of the Supplicant (set *reAuthEnabled* equal to TRUE).
21. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
22. Attempt to access services located on the LAN connected to the DUT.

Part F: AuthControlledPortControl set to ForceUnauthorized

23. Ensure that the default test layout is connected and configured properly.
24. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
25. Configure *AuthControlledPortControl* parameter on the DUT with a value equal to *ForceUnauthorized*.
26. Attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In step 3, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 8, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.
- In step 12, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.
- In step 17, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 22, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 26, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.

Possible Problems:

- In steps 8 and 12, if the Supplicant is configured for automatic re-authentication (via cached credentials), an observation via LT of an Authentication process will be sufficient to pass the tests. An observation between the DUT and a supplicant should appear in this order:
    1. DUT sends EAP Request for Identity
    2. DUT receives EAP Response with Identity (from supplicant)
    3. DUT sends EAP Request for Credentials (via MD5-Challenge)
    4. DUT receives EAP Response with Credentials (via MD5-Challenge from supplicant)
    5. DUT sends EAP Success
- In Part E, this test is Not Applicable (N/A), if the DUT does not support the ability to configure the *reAuthEnabled* parameter.

802.1X.io.2.2: Basic Interoperability - PEAP

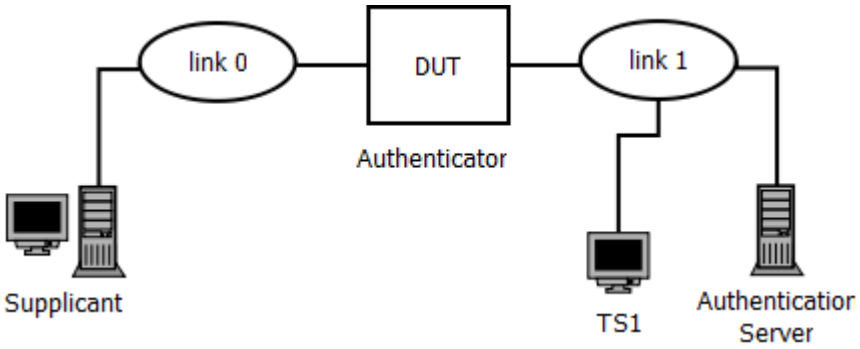
Purpose: To verify that the DUT, assuming the Authenticator role, can properly authenticate the credentials of a variety of Supplicants, using the PEAP authentication method.

References:

- IEEE Std 802.1X-2004
  - Sub-clause 5.1 – Static conformance requirements
  - Sub-clause 6.6.4 – Logoff mechanisms
  - Sub-clause 8.2.8 – Reauthentication Timer state machine
- draft-josefsson-pppext-eap-tls-eap-08
- RFC-2284 – EAP
- RFC-2865 – RADIUS

Discussion:

This test verifies that the DUT can properly authenticate the Supplicant's credentials, thereby allowing the Supplicant access to services offered by the LAN to which the DUT is attached. The Supplicant's credentials are authenticated by the Authentication Server via the DUT. Once the DUT has received an authentication accept message, from the Authentication Server, the Controlled Port, of the Port on the DUT connected to the Supplicant, is placed in the *authorized* state.



Procedure:

Part A: Basic Interoperability

1. Ensure that the default test layout is connected and configured properly.
2. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
3. Attempt to access services located on the LAN connected to the DUT.

Part B: Aging out of the authorization state (set reAuthPeriod equal to 300)

4. Ensure that the default test layout is connected and configured properly.
5. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
6. Configure the *reAuthPeriod* parameter on the DUT equal to a value of 300 seconds.
7. Wait more than 300 seconds (5 minutes).
8. Attempt to access services located on the LAN connected to the DUT.

Part C: Link loss between Supplicant and Authenticator

9. Ensure that the default test layout is connected and configured properly.
10. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
11. Disconnect/reconnect the link between the Supplicant and the DUT.
12. Attempt to access services located on the LAN connected to the DUT.

Part D: Authenticator Re-initialization

13. Ensure that the default test layout is connected and configured properly.
14. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
15. Reboot the DUT (Authenticator).

16. Allow time for the DUT to initialize and for the Supplicant to become authenticated by the Authentication Server via the DUT.
17. Attempt to access services located on the LAN connected to the DUT.

Part E: Reauthentication while in authenticated state (set reAuthEnabled equal to TRUE)

18. Ensure that the default test layout is connected and configured properly.
19. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
20. Use DUT to initiate reauthentication of the Supplicant (set *reAuthEnabled* equal to TRUE).
21. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
22. Attempt to access services located on the LAN connected to the DUT.

Part F: AuthControlledPortControl set to ForceUnauthorized

23. Ensure that the default test layout is connected and configured properly.
24. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
25. Configure *AuthControlledPortControl* parameter on the DUT with a value equal to *ForceUnauthorized*.
26. Attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In step 3, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 8, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.
- In step 12, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.
- In step 17, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 22, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 26, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.

Possible Problems:

- In steps 8 and 12, if the Supplicant is configured for automatic re-authentication (via cached credentials), an observation via LT of an Authentication process will be sufficient to pass the tests. An observation between the DUT and a supplicant should appear in this order:
    1. DUT sends EAP Request for Identity
    2. DUT receives EAP Response with Identity (from supplicant)
    3. DUT sends EAP Request for Credentials (via PEAP)
    4. DUT receives EAP Response with Credentials (via PEAP from supplicant)
    5. DUT sends EAP Success
- In Part E, this test is Not Applicable (N/A), if the DUT does not support the ability to configure the *reAuthEnabled* parameter.

802.1X.io.2.3: Basic Interoperability - TTLS

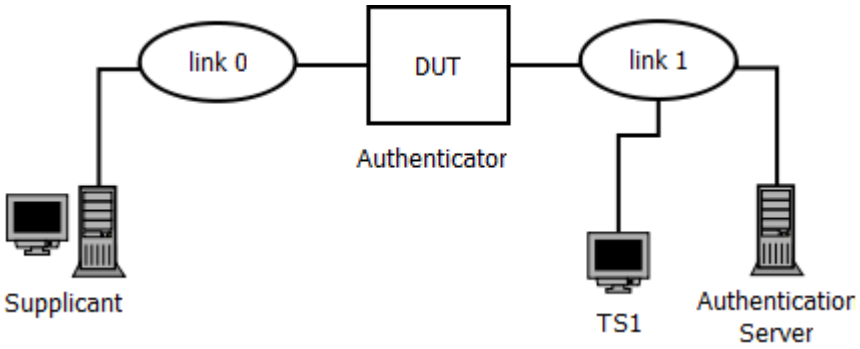
Purpose: To verify that the DUT, assuming the Authenticator role, can properly authenticate the credentials of a variety of Supplicants, using the TTLS authentication method.

References:

- IEEE Std 802.1X-2004
  - Sub-clause 5.1 – Static conformance requirements
  - Sub-clause 6.6.4 – Logoff mechanisms
  - Sub-clause 8.2.8 – Reauthentication Timer state machine
- draft-ietf-pppext-eap-ttls-05
- RFC-2284 – EAP
- RFC-2865 – RADIUS

Discussion:

This test verifies that the DUT can properly authenticate the Supplicant's credentials, thereby allowing the Supplicant access to services offered by the LAN to which the DUT is attached. The Supplicant's credentials are authenticated by the Authentication Server via the DUT. Once the DUT has received an authentication accept message, from the Authentication Server, the Controlled Port, of the Port on the DUT connected to the Supplicant, is placed in the *authorized* state.



Procedure:

Part A: Basic Interoperability

1. Ensure that the default test layout is connected and configured properly.
2. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
3. Attempt to access services located on the LAN connected to the DUT.

Part B: Aging out of the authorization state (set reAuthPeriod equal to 300)

4. Ensure that the default test layout is connected and configured properly.
5. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
6. Configure the *reAuthPeriod* parameter on the DUT equal to a value of 300 seconds.
7. Wait more than 300 seconds (5 minutes).
8. Attempt to access services located on the LAN connected to the DUT.

Part C: Link loss between Supplicant and Authenticator

9. Ensure that the default test layout is connected and configured properly.
10. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
11. Disconnect/reconnect the link between the Supplicant and the DUT.
12. Attempt to access services located on the LAN connected to the DUT.

Part D: Authenticator Re-initialization

13. Ensure that the default test layout is connected and configured properly.
14. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
15. Reboot the DUT (Authenticator).

16. Allow time for the DUT to initialize and for the Supplicant to become authenticated by the Authentication Server via the DUT.
17. Attempt to access services located on the LAN connected to the DUT.

Part E: Reauthentication while in authenticated state (set reAuthEnabled equal to TRUE)

18. Ensure that the default test layout is connected and configured properly.
19. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
20. Use DUT to initiate reauthentication of the Supplicant (set *reAuthEnabled* equal to TRUE).
21. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
22. Attempt to access services located on the LAN connected to the DUT.

Part F: AuthControlledPortControl set to ForceUnauthorized

23. Ensure that the default test layout is connected and configured properly.
24. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
25. Configure *AuthControlledPortControl* parameter on the DUT with a value equal to *ForceUnauthorized*.
26. Attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In step 3, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 8, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.
- In step 12, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.
- In step 17, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 22, the Supplicant should be able to access services located on the LAN connected to the DUT.
- In step 26, the Supplicant should **not** be able to access services located on the LAN connected to the DUT.

Possible Problems:

- In steps 8 and 12, if the Supplicant is configured for automatic re-authentication (via cached credentials), an observation via LT of an Authentication process will be sufficient to pass the tests. An observation between the DUT and a supplicant should appear in this order:
    1. DUT sends EAP Request for Identity
    2. DUT receives EAP Response with Identity (from supplicant)
    3. DUT sends EAP Request for Credentials (via TTLS)
    4. DUT receives EAP Response with Credentials (via TTLS from supplicant)
    5. DUT sends EAP Success
- In Part E, this test is Not Applicable (N/A), if the DUT does not support the ability to configure the *reAuthEnabled* parameter.

GROUP 3: Extended 802.1X Interoperability

Scope

The following tests are designed to verify the extended interoperability functions of 802.1X capable devices.

Overview

The tests in this group verify that all the components of the 802.1X capable LAN are interoperating properly, extended beyond the basic functions of 802.1X. In these tests the DUT is placed in varying test setups to examine its behavior.

802.1X.io.3.1: Multi-Supplicant Interoperability

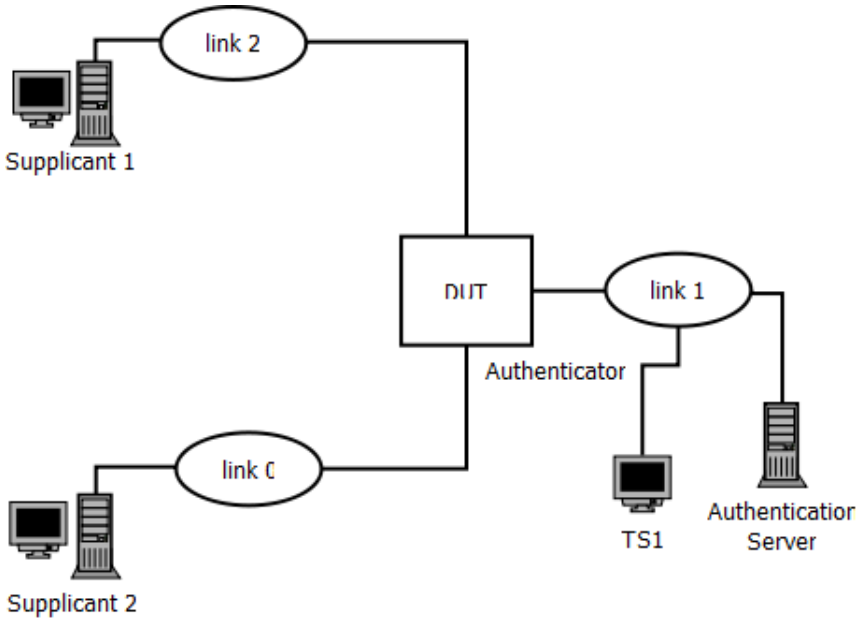
Purpose: To verify that the DUT, assuming the Authenticator role, can properly authenticate the credentials of a variety of Supplicants while not blocking/affecting the ability of other Supplicants, connected to the DUT via Ports whose Controlled Port is in the *ForceAuthorized* state, to access services in the LAN connected to the DUT.

References:

- IEEE Std 802.1X-2004
- draft-josefsson-pppext-eap-tls-eap-08
- draft-ietf-pppext-eap-ttls-05
- RFC-2284 – EAP
- RFC-2716 – EAP-TLS
- RFC-2865 – RADIUS

Discussion:

This Test verifies that the DUT can properly authenticate a Supplicant's credentials and provide access to services located on the LAN connected to the DUT, while not blocking/affecting the ability of other Supplicants that are connected to the DUT to access these services.



Procedure:

Part A: Multi-Supplicant Interoperability

1. Ensure that the default test layout is connected and configured properly.
2. Allow time for the Supplicants to become authenticated by the Authentication Server via the DUT.
3. Use both Supplicants to attempt to access services located on the LAN connected to the DUT.
4. Repeat this test using all available Supplicants.

Observable Results:

- In step 4, both Supplicants should be able to access services located on the LAN connected to the DUT.

Possible Problems:

- None.

802.1X.io.3.2: Port disabled via management

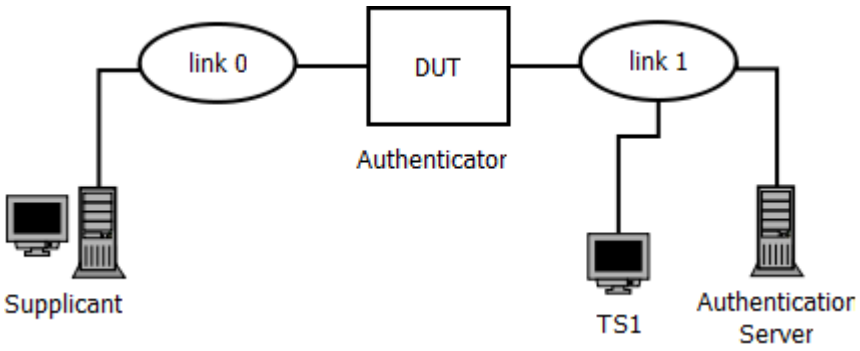
Purpose: To verify that the DUT, assuming the Authenticator role, does not change the state of a Port disabled via management when authenticating the credentials of a variety of Supplicants.

References:

- IEEE Std 802.1X-2004
- IEEE Std 802.1D-2004
  - Sub-clause 6.4.2 – MAC status parameters
- RFC-2284 – EAP
- RFC-2865 – RADIUS

Discussion:

This test verifies that the operation of 802.1X on the DUT does not change the Administrative controls when attempting to authenticate the Supplicant's credentials.



Test Specific Setup:

- In Part A, configure the *MAC_Enabled* parameter on the Port on the DUT connected to Supplicant to have a value of FALSE.

Procedure:

Part A: Port Disabled

1. Ensure that the default test layout is connected and configured properly.
2. Allow time for the Supplicants to attempt to become authenticated by the Authentication Server via the DUT.
3. Attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In step 3, the Supplicant should **not** be able to access services located on the LAN connected to the DUT. The DUT should not modify the value of the *MAC_Enabled* parameter on the Port on the DUT connected to the Supplicant.

Possible Problems:

- None.

802.1X.io.3.3: Interoperability within a VLAN Environment

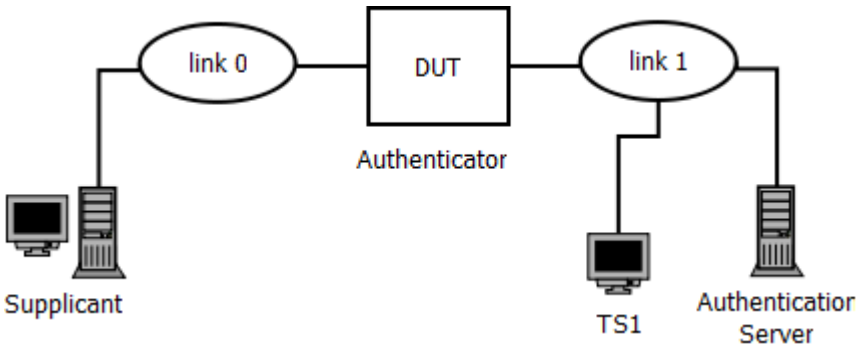
Purpose: To verify that the DUT, assuming the Authenticator role, can properly authenticate the credentials of a Supplicant over a specific VLAN other than the default.

References:

- IEEE Std 802.1X-2004
- IEEE Std 802.1Q-2003
- RFC-2284 – EAP
- RFC-2865 – RADIUS

Discussion:

This test verifies that the DUT can properly authenticate the credentials of a Supplicant over a VLAN other than the default VLAN, thereby allowing the Supplicant access to services offered by the LAN to which the DUT is attached. Once the DUT has authenticated the Supplicant, its ability to access services on the LAN will be verified.



Procedure:

Part A: VLAN Environment

1. Ensure that the default test layout is connected and configured properly.
2. Configure the port connected to the Authentication Server to be an untagged member of VLAN 64.
3. Configure the port connected to the Supplicant to be an untagged member of VLAN 64.
4. Allow time for the Supplicant to become authenticated by the Authentication Server via the DUT.
5. Attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In step 5, the Supplicant should be able to access services located in VLAN 64 in the LAN connected to the DUT.

Possible Problems:

- If the DUT does not support VLANs, this test cannot be completed.

GROUP 4: Basic Security

Scope

The following tests are designed to test some of the basic security features of the 802.1X security protocols.

Overview

The tests in this group use Good, Bad, and Ugly credentials.

- A set of Good Credentials is valid and can be correctly authenticated by the Authentication Server.
- A set of Bad Credentials has a correct username and/or certificate, but either has an invalid password or the certificate is expired.
- A set of Ugly Credentials has neither a correct username nor a correct certificate.

Only the set of Good credentials should be authenticated. The sets of Bad and Ugly credentials should be put in the *Unauthorized* state.

Note: *If the DUT failed part A of any tests in Group 2, the relative test in this group will not be run as the DUT has failed basic interoperability with that authentication mechanism.*

802.1X.io.4.1: Basic Security over MD5-Challenge (EAP-MD5)

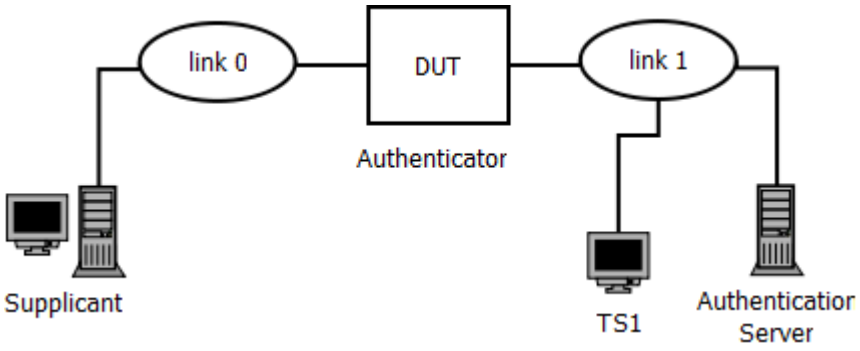
Purpose: To verify that the DUT, assuming the Authenticator role, only puts the Port connected to the Supplicant in an *Authorized* state if valid credentials are received. If invalid credentials are received the Port should be put into the *Unauthorized* state.

References:

- IEEE Std 802.1X-2004
- RFC-1321 – MD5
- RFC-2284 – EAP
- RFC-2865 – RADIUS

Discussion:

This Test verifies that the DUT will properly authenticate a Supplicant's credentials and provide access to services located on the LAN connected to the DUT if the credentials are good. If the credentials are invalid it will not allow access to services located on the LAN. This test has been deprecated.



Procedure:

Part A: Good Credentials

1. Ensure that the default test layout is connected and configured properly.
2. When initializing the Supplicant software, use a correct Username and Password combination that is known by the Authenticator and Authentication Server that lead to the port being in an *Authorized* state.
3. Attempt to access services located on the LAN connected to the DUT.

Part B: Bad Credentials

4. Ensure that the default test layout is connected and configured properly.
5. When initializing the Supplicant software, use a Username known to the Authenticator and Authentication Server but **not** the Password that corresponds with the Username.
6. Attempt to access services located on the LAN connected to the DUT.

Part C: Ugly Credentials

7. Ensure that the default test layout is connected and configured properly.
8. When initializing the Supplicant software, use a Username and Password combination that is **not** known to the Authenticator or Authentication Server.
9. Attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In step 3, the Supplicant should be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Authorized* state.
- In step 6, the Supplicant should **not** be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Unauthorized* state.

- In step 9, the Supplicant should **not** be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Unauthorized* state.

Possible Problems:

- None.

802.1X.io.4.2: Basic Security over PEAP

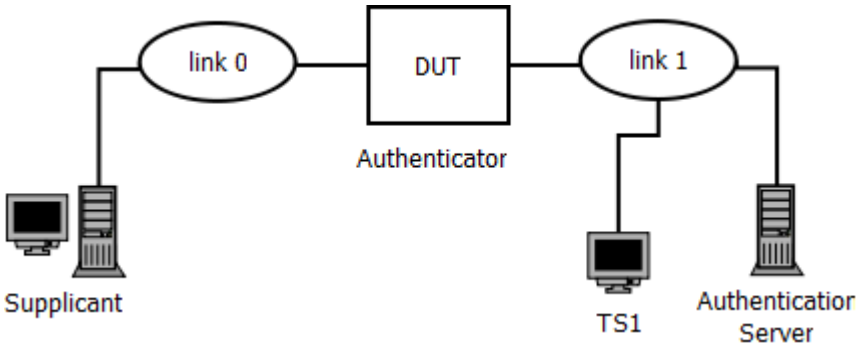
Purpose: To verify that the DUT, assuming the Authenticator role, only puts the Port connected to the Supplicant in an *Authorized* state if valid credentials are received. If invalid credentials are received the Port should be put into the *Unauthorized* state.

References:

- IEEE Std 802.1X-2004
- draft-josefsson-pppext-eap-tls-eap-08
- RFC-2284 – EAP
- RFC-2865 – RADIUS

Discussion:

This Test verifies that the DUT will properly authenticate a Supplicant's credentials and provide access to services located on the LAN connected to the DUT if the credentials are good. If the credentials are invalid it will not allow access to services located on the LAN.



Procedure:

Part A: Good Credentials

1. Ensure that the default test layout is connected and configured properly.
2. When initializing the Supplicant software, use a correct Username and Password combination that is known by the Authenticator and Authentication Server that lead to the port being in an *Authorized* state.
3. Attempt to access services located on the LAN connected to the DUT.

Part B: Bad Credentials

4. Ensure that the default test layout is connected and configured properly.
5. When initializing the Supplicant software, use a Username known to the Authenticator and Authentication Server but **not** the Password that corresponds with the Username.
6. Attempt to access services located on the LAN connected to the DUT.

Part C: Ugly Credentials

7. Ensure that the default test layout is connected and configured properly.
8. When initializing the Supplicant software, use a Username and Password combination that is **not** known to the Authenticator or Authentication Server.
9. Attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In Part A, the Supplicant should be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Authorized* state.
- In Part B, the Supplicant should **not** be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Unauthorized* state.

- In Part C, the Supplicant should **not** be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Unauthorized* state.

Possible Problems:

- None.

802.1X.io.4.3: Basic Security over TTLS

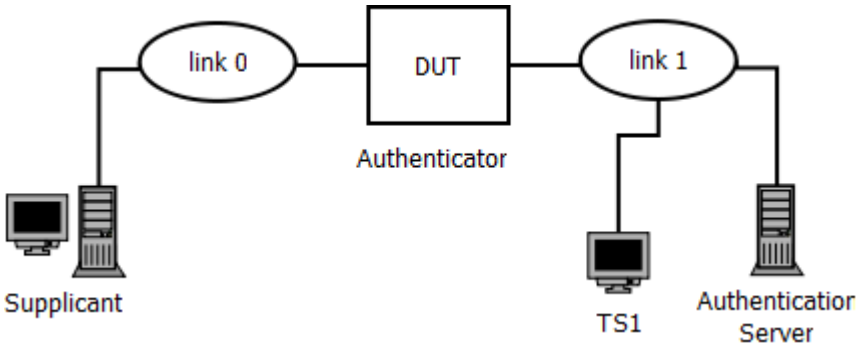
Purpose: To verify that the DUT, assuming the Authenticator role, only puts the Port connected to the Supplicant in an *Authorized* state if valid credentials are received. If invalid credentials are received the Port should be put into the *Unauthorized* state.

References:

- IEEE Std 802.1X-2004
- draft-ietf-pppext-eap-ttls-05
- RFC-2284 – EAP
- RFC-2865 – RADIUS

Discussion:

This Test verifies that the DUT will properly authenticate a Supplicant's credentials and provide access to services located on the LAN connected to the DUT if the credentials are good. If the credentials are invalid it will not allow access to services located on the LAN.



Procedure:

Part A: Good Credentials

1. Ensure that the default test layout is connected and configured properly.
2. When initializing the Supplicant software, use a correct Username and Password combination that is known by the Authenticator and Authentication Server that lead to the port being in an *Authorized* state.
3. Attempt to access services located on the LAN connected to the DUT.

Part B: Bad Credentials

4. Ensure that the default test layout is connected and configured properly.
5. When initializing the Supplicant software, use a Username known to the Authenticator and Authentication Server but **not** the Password that corresponds with the Username.
6. Attempt to access services located on the LAN connected to the DUT.

Part C: Ugly Credentials

7. Ensure that the default test layout is connected and configured properly.
8. When initializing the Supplicant software, use a Username and Password combination that is **not** known to the Authenticator or Authentication Server.
9. Attempt to access services located on the LAN connected to the DUT.

Observable Results:

- In Part A, the Supplicant should be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Authorized* state.
- In Part B, the Supplicant should **not** be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Unauthorized* state.

- In Part C, the Supplicant should **not** be able to access services located on the LAN connected to the DUT and the Port connected to the Supplicant should be in the *Unauthorized* state.

Possible Problems:

- None.