Bridge Functions Consortium

Port-Based Network Access Control
802.1X Supplicant Conformance Test Suite
Version 1.2

Last Updated: 2008-02-14

Bridge Functions Consortium
University of New Hampshire
Research Computing Center
InterOperability Laboratory

121 Technology Drive, Suite 2
Durham, NH 03824
Phone: (603) 862-0090
Fax: (603) 862-4181
www.iol.unh.edu

TABLE OF CONTENTS

MODIFICATION RECORD

Version	Date	Editor(s)	Comments
0.1	2006-01-09	Andrew Corcoran Tyler Marcotte	Initial Design for IEEE Std. 802.1X™-2001
0.2	2006-03-10	Andrew Corcoran Jeremy deVries Tyler Marcotte	Completed addition of Tests for all Groups.
0.3	2006-03-14	Tyler Marcotte	Review and revision.
0.4	2006-03-28	Tyler Marcotte	Review and revision (frames)
1.0	2006-06-23	Tyler Marcotte	Review and revision. Renamed frames.
1.2	2008-02-14	Corey Hill	Updated for 802.1X™-2004

ACKNOWLEDGEMENTS

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

Andrew Corcoran	UNH InterOperability Laboratory
Jeremy deVries	UNH InterOperability Laboratory
Tyler Marcotte	UNH InterOperability Laboratory
Curtis Simonson	UNH InterOperability Laboratory
Corey Hill	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 802.1X 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. supplicant configuration time, device startup time, 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 interoperability tests. Rather, they provide one method to isolate problems within an 802.1X 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 802.1X 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 802.1X capable environments.

[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"

[RFC-2284] Blunk & Vollbrecht, "PPP Extensible Authentication Protocol (EAP)"

[IEEE Std 802.1Q™-2003] IEEE Computer Society LAN/MAN Standards Committee, "Virtual Bridged Local Area Networks"

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
MAC	Media Access Control
PAE	Port Access Entity
Port	Network Access Port
RADIUS	Remote Authentication Dial in User Service
TS	Test Station

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.
DUT	An 802.1X capable supplicant system.
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.
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.
Supplicant PAE	The Supplicant PAE is responsible for responding to requests from an Authenticator for information that will establish its credentials.

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-Supp.op.1.2 refers to the second test of the first test group in the 802.1X Supplicant Operations 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.

Resource Requirements: The Resource Requirements section specifies the software, hardware, and test equipment that will be needed to perform the test. 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.

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.

Test Layout: This diagram shows how the Test Systems, DUT, and any other Devices used should be connected for this test. Elements of the Procedure may change the Layout.

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.

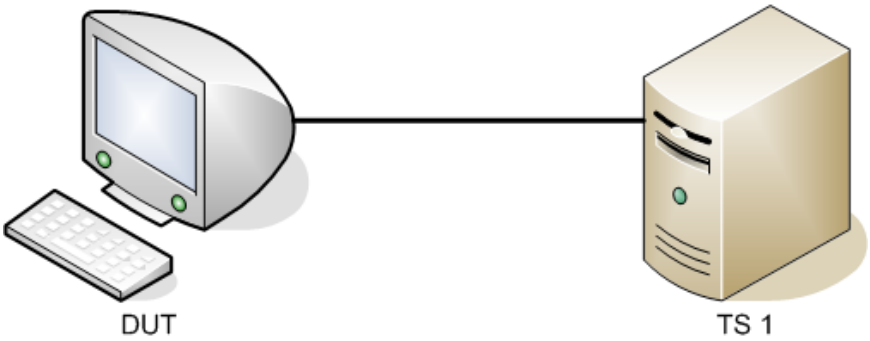
Observable Results: This section lists observable results that can be examined by the tester to verify that the DUT is operating properly. When multiple observable results are possible, this section provides a short discussion on how to interpret them. The determination of a PASS or FAIL for each test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

Default Settings: DUT

802.1X SystemAuthControl	Disabled
authPeriod	30 seconds
heldPeriod	60 seconds
startPeriod	30 seconds
maxStart	3
suppStatus	Unauthorized
userLogoff	false
VLAN Tagging	Disabled



GROUP 1: System Configuration Functions

Scope

To verify that the DUT supports the proper System Configuration Functions as specified in IEEE 802.1X-2001 sub-clause 9.6.

Overview

This Group tests the following parameters:

- System Read Function
- System Set Function
- System Initialize Function

802.1X-Supp.op.1.1 : System Read Function

Purpose: To verify the DUT supports the proper system read functions and provides the correct values when the read functions are exercised.

References:

- IEEE Std. 802.1X-2004: sub-clause 9.6.1.1

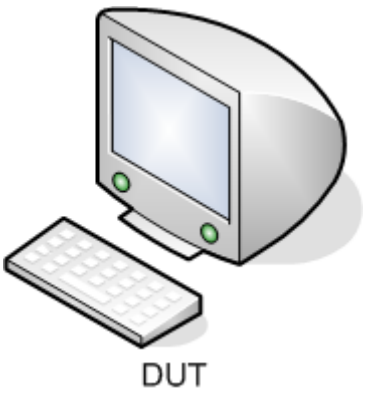
Resource Requirements:

- None.

Discussion:

The System Configuration managed object models the operations that modify, or enquire about, the configuration of the System's resources. There is a single System Configuration managed object for each System that supports Port Access Control functionality. The first of three management operations that can be performed on the System Configuration managed object is the Read System Configuration operation, whose purpose is to read the configuration information associated with the System.

Test Layout:



Procedure:

Part A: Read System Configuration

1. Ensure that the default values are configured on the DUT.
2. Attempt to extract the System Configuration from the device via management.

Observable Results:

- In step 2, the DUT should report the SystemAuthControl parameter for the System. This parameter should have the value of Disabled.
- In step 2, for each port of the system, the DUT should report:
    1. The Port number assigned to the Port by the System in which the Port resides.
    2. The Protocol version number of the EAPOL implementation supported by the Port.
    3. The capabilities of the PAE associated with the Port.

Possible Problems:

- If the DUT does not support configuration via management, this Test cannot be completed.

802.1X-Supp.op.1.2 : System Set Function

Purpose: To verify the DUT supports the proper system set function and does not accept configuration of invalid values when the set function is exercised.

References:

- IEEE Std. 802.1X-2004: sub-clause 9.6.1.2

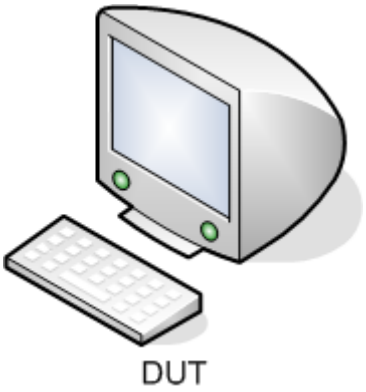
Resource Requirements:

- None.

Discussion:

The System Configuration managed object models the operations that modify, or enquire about, the configuration of the System's resources. There is a single System Configuration managed object for each System that supports Port Access Control functionality. The second of three management operations that can be performed on the System Configuration managed object is the Set System Configuration operation, whose purpose is to set the configuration information associated with the System.

Test Layout:



Procedure:

Part A: Set System Configuration

1. Ensure that the default values are configured on the DUT.
2. Attempt to set the SystemAuthControl parameter for the DUT to "Enabled".
3. Attempt to set the SystemAuthControl parameter for the DUT to "Disabled".

Observable Results:

- In step 2, the DUT should accept the configuration change with the value of "Enabled".
- In step 3, the DUT should accept the configuration change with the value of "Disabled".

Possible Problems:

- If the DUT does not support configuration via management this Test cannot be completed.

802.1X-Supp.op.1.3 : Initialize Port

Purpose: To verify the DUT supports the proper system initial functions and does not accept configuration of invalid values when the initialize function is exercised.

References:

- IEEE Std. 802.1X-2004: sub-clause 9.6.1.3

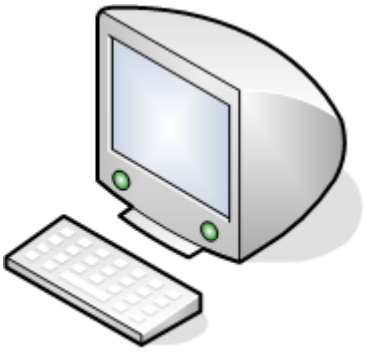
Resource Requirements:

- None.

Discussion:

The System Configuration managed object models the operations that modify, or enquire about, the configuration of the System's resources. There is a single System Configuration managed object for each System that supports Port Access Control functionality. The last of three management operations that can be performed on the System Configuration managed object is the Initialize Port operation, whose purpose is to cause the EAPOL state machines for the Port to be initialized.

Test Layout:



Procedure:

Part A: Initialize Port

1. Ensure that the default values are configured on the DUT.
2. Attempt to set the SystemAuthControl parameter for the DUT to the value of "Enabled".

Observable Results:

- In step 2, the DUT should accept the configuration change with the value of "Enabled".
- In step 2, if the Port state is down, the current state of the DUT should be observed via management as "DISCONNECTED".
- In step 2, if the Port state is up, the current state of the DUT should be observed via management as "CONNECTING".

Possible Problems:

- If the DUT does not support configuration via management, this Test cannot be completed.

GROUP 2: Supplicant Configuration Functions

Scope

To verify that the DUT supports the proper Supplicant Configuration Functions as specified in IEEE 802.1X-2001 sub-clause 9.5.

Overview

This Group tests the following functions:

- Supplicant Read Function
- Supplicant Set Function

802.1X-Supp.op.2.1 : Read Supplicant Status

Purpose: To verify that the DUT supports the proper Supplicant read functions and provides the correct values when the read functions are exercised.

References:

- IEEE Std. 802.1X-2004: sub-clause 9.5.1.1

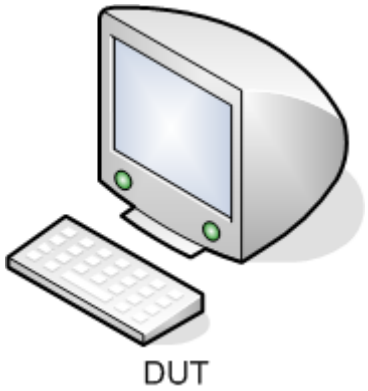
Resource Requirements:

- None.

Discussion:

The Supplicant Configuration managed object models the operations that modify, or inquire about, the configuration of the Supplicant's resources. There is a single Supplicant Configuration managed object for each Port that supports Supplicant functionality. The first management operation that can be performed on the Supplicant Configuration managed object is the Read Supplicant Status operation.

Test Layout:



Procedure:

Part A: Read Supplicant Status

1. Ensure that the default values are configured on the DUT.
2. Attempt to extract the Supplicant status of a Port on the DUT for which Supplicant PAE functionality is supported.

Observable Results:

- The DUT should report the following information for the Port:
  - The identification number assigned to the Port by the System in which the port resides.
  - The current state of the Supplicant PAE state machine. This parameter can be one of the following: DISCONNECTED, LOGOFF, CONNECTING, AUTHENTICATING, AUTHENTICATED, RESTART, HELD.
  - The value of the heldPeriod constant currently used by the Supplicant state machine.
  - The value of the authPeriod constant currently used by the Supplicant state machine.
  - The value of the startPeriod constant currently used by the Supplicant state machine.
  - The value of the maxStart constant currently used by the Supplicant state machine.

Possible Problems:

- If the DUT does not support configuration via management, then the Test cannot be completed.

802.1X-Supp.op.2.2 : Set Supplicant Configuration

Purpose: To verify that the DUT supports the proper supplicant configuration functions.

References:

- IEEE Std. 802.1X-2004: sub-clause 9.5.1.2

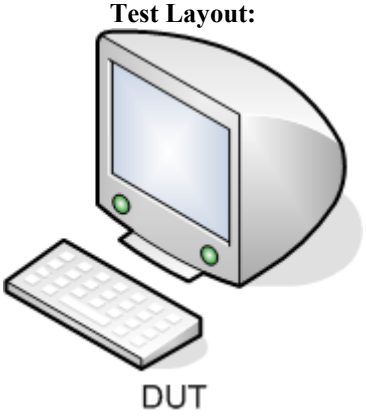
Resource Requirements:

- None.

Discussion:

The Supplicant Configuration managed object models the operations that modify, or enquire about, the configuration of the Supplicant's resources. There is a single Supplicant Configuration managed object for each Port that supports Supplicant functionality. The second management operation that can be performed on the Supplicant Configuration managed object is the Set Supplicant Configuration operation.

Test Layout:



Procedure:

Part A: Set Supplicant Configuration

1. Ensure that the default values are configured on the DUT.
2. Attempt to set the heldPeriod constant for a Port on the DUT that supports Supplicant PAE functionality to a non-default value.
3. Attempt to set the authPeriod constant to for a Port on the DUT that supports Supplicant PAE functionality to a non-default value.
4. Attempt to set the startPeriod constant for a Port on the DUT that supports Supplicant PAE functionality to a non-default value.
5. Attempt to set the maxStart constant for a Port on the DUT that supports Supplicant PAE functionality to a non-default value.
6. Attempt to extract Supplicant status for the Port on the DUT on which the configuration changes were committed.

Observable Results:

- The Supplicant status for the Port on the DUT that the configuration changes were committed will reflect the changes for the heldPeriod, authPeriod, startPeriod, and maxStart constants.

Possible Problems:

- If the DUT does not support configuration via management, this Test cannot be completed.
- If the DUT does not support the configuration of the heldPeriod, authPeriod, startPeriod, or maxStart constants, this Test cannot be completed.

GROUP 3: EAPOL Frame Format Validation

Scope

This group of tests verifies that the DUT uses the proper Frame Format when transmitting EAPOL packets.

Overview

This group tests three different types of EAPOL frames.

- EAPOL-Start
- EAPOL-EAP
- EAPOL-Logoff

802.1X-Supp.op.3.1: EAPOL Start Frame Validation

Purpose: This test verifies that an EAPOL Frame of type Start transmitted by the DUT is properly formatted.

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: Figure 7-1

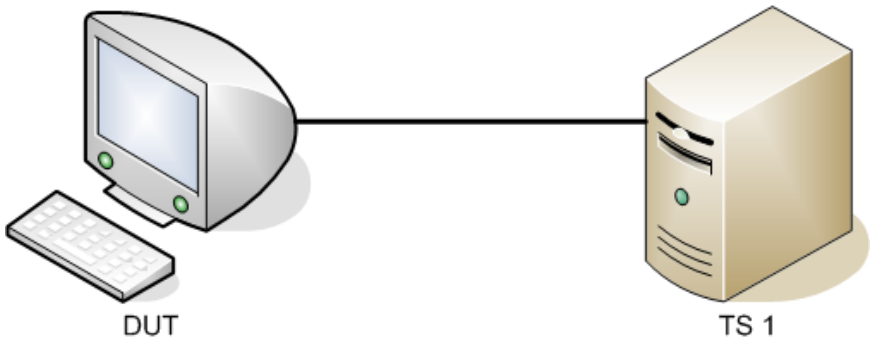
Resource Requirements:

- 1 Test Station

Discussion:

An EAPOL Start frame is used to notify an Authenticator that an 802.1X capable device has connected to a port on the Authenticator. After an EAPOL Start frame is received by the Authenticator, the 802.1X authentication process is initialized by the Authenticator and Supplicant walking through their respective state machines.

Test Layout:



Procedure:

Part A: EAPOL Start Frame Validation

1. Ensure that the default values are configured on the DUT.
2. Start capture on Test Station 1.
3. Set the SystemAuthControl parameter on the DUT to "Enabled".
4. Wait 30 seconds.
5. Stop capture on Test Station 1 and observe the captured frames (if any).

Observable Results:

- Test Station 1 should capture at least one EAPOL Start frame. These frames must contain the following parameter values:

Destination Address:	0x0180C2000003
Source Address:	0x001234567890 (Must be equal to the MAC Address assigned to the DUT)
PAE Ethernet Type:	0x888E
Protocol Version:	0x01
Packet Type:	0x01
Packet Body Length:	0x00

Possible Problems:

- None.

802.1X-Supp.op.3.2: EAPOL Logoff Frame Validation

Purpose: This test verifies that an EAPOL frame of type Logoff transmitted by the DUT is properly formatted.

References:

- IEEE Std. 802.1X-2004: sub-clause 6.6.4
- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.5

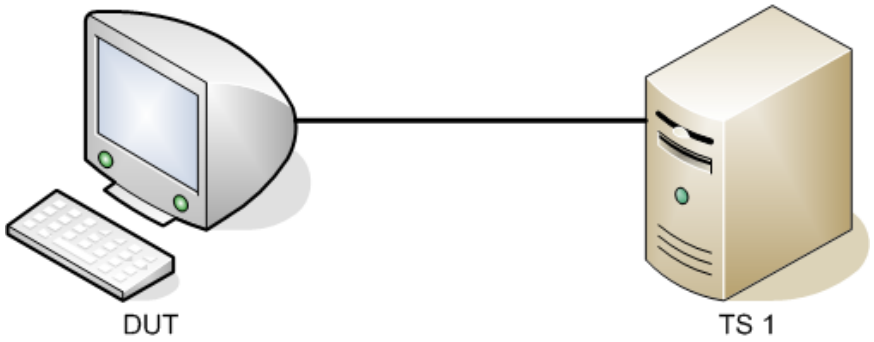
Resource Requirements:

- 1 Test Station

Discussion:

An EAPOL Logoff frame is used to indicate that a user has enabled a parameter or disabled the supplicant. This frame is triggered by having the userLogoff variable set to TRUE.

Test Layout:



Procedure:

Part A: EAPOL Logoff Frame Validation

1. Ensure that the default values are configured on the DUT.
2. Start capture on Test Station 1.
3. Set the SystemAuthControl parameter on the DUT to "Enabled".
4. Wait 60 Seconds.
5. Restart the Authentication mechanism on the DUT.
6. Wait 60 Seconds.
7. Set the SystemAuthControl parameter on the DUT to "Disabled".
8. Stop capture on Test Station 1 and observe the captured frames (if any).

Observable Results:

- Test Station 1 should capture at least one EAPOL Logoff frame. These frames must contain the following parameter values:

Destination Address:	0x0180C2000003
Source Address:	0x001234567890 (Must be equal to the MAC Address assigned to the DUT)
PAE Ethernet Type:	0x888E
Protocol Version:	0x01
Packet Type:	0x02
Packet Body Length:	0x00

Possible Problems:

- None.

802.1X-Supp.op.3.3: EAPOL EAP Response Identity Frame Validation

Purpose: This test verifies that an EAPOL frame containing an EAP Response of type Identity transmitted by the DUT is properly formatted.

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

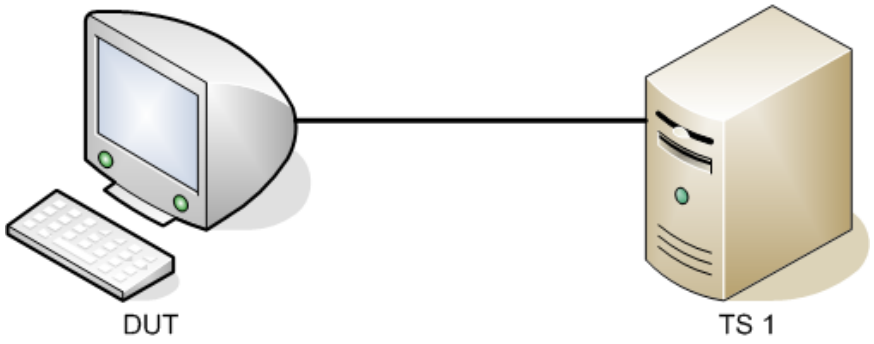
Resource Requirements:

- 1 Test Station

Discussion:

As part of the authentication process involved in 802.1X, an EAP Response of type Identity will be sent from the Supplicant to the Authenticator. This response provides an identity (i.e. a username or certificate owner) of the Supplicant. This is then transmitted to the Authentication Server via the Authenticator so that it may look up and cross-reference the rest of the credentials that will be transmitted later in the authentication process.

Test Layout:



Procedure:

Part A: EAPOL EAP Response Identity

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl parameter on the DUT to "Enabled".
3. Start capture on Test Station 1
4. Transmit a RequestSupplicantIdentity frame from Test Station 1.
5. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
6. Stop capture on Test Station 1 and observe the captured frames (if any).

Observable Results:

- Test Station 1 must capture at least one EAPOL EAP Response frame. This frame must contain the following parameter values:

Destination Address:	0x0180C2000003
Source Address:	0x001234567890 (Must be equal to the MAC Address assigned to the DUT)
PAE Ethernet Type:	0x888E
Protocol Version:	0x01
Packet Type:	0x00
Packet Body Length:	0x0009 (This is variable depending on the EAP Type-Data received)
EAP Code:	0x02
EAP Identifier:	0x01
EAP Length:	0x0009 (This must be equal to the Packet Body Length)
EAP Type:	0x01
EAP Type-Data:	(There should be an ASCII representation of the username submitted by the DUT)

Possible Problems:

- None.

802.1X-Supp.op.3.4: EAPOL EAP Response Nak Frame Validation

Purpose: This test verifies that an EAPOL frame that contains an EAP Response frame of type Nak transmitted by the DUT is properly formatted.

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

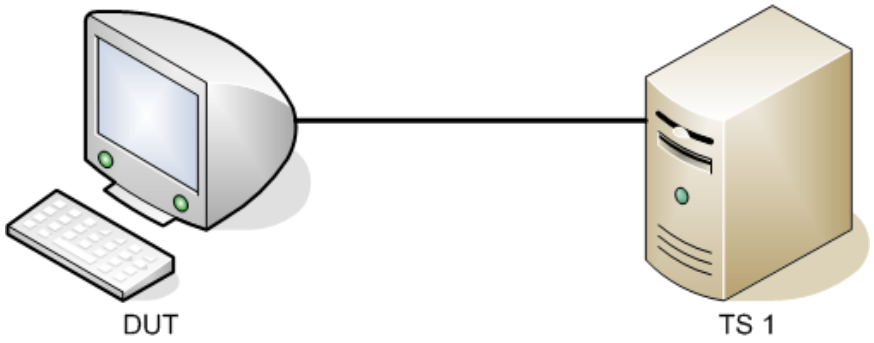
Resource Requirements:

- 1 Test Station

Discussion:

An EAP Response frame of type Nak is sent when a request for authentication asks to use an Authenticaiton mechanism that is not supported. The Supplicant has the option of adding information about which authentication mechanism it would like to use. If the Supplicant chooses to do this, it is added in the Type-Data field of the response packet.

Test Layout:



Procedure:

Part A: EAPOL EAP Response Nak

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl parameter on the DUT to "Enabled".
3. Start capture on Test Station 1.
4. Transmit a RequestForUnknownMechanism frame from Test Station 1.
5. Stop capture on Test Station 1 and observe the captured frames (if any).

Observable Results:

- Test Station 1 must capture at least one EAPOL Response frame. This frame must contain the following parameter values:

Destination Address:	0x0180C2000003
Source Address:	0x001234567890 (Must be equal to the MAC Address assigned to the DUT)
PAE Ethernet Type:	0x888E
Protocol Version:	0x01
Packet Type:	0x00
Packet Body Length:	0x0006
EAP Code:	0x02
EAP Identifier:	0x01
EAP Length:	0x0006
EAP Type:	0x03
EAP Type-Data:	0x04 (This should be the Type that the DUT wishes to use for Authentication)

Possible Problems:

- If the default value for EAP Type is supported, a different value that is not supported should be substituted in its place when transmitting the request.

802.1X-Supp.op.3.5: EAPOL EAP Response MD5 Frame Validation

Purpose: This test verifies that an EAPOL frame that contains an EAPOL EAP Response frame of type MD5 transmitted by the DUT is properly formatted.

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

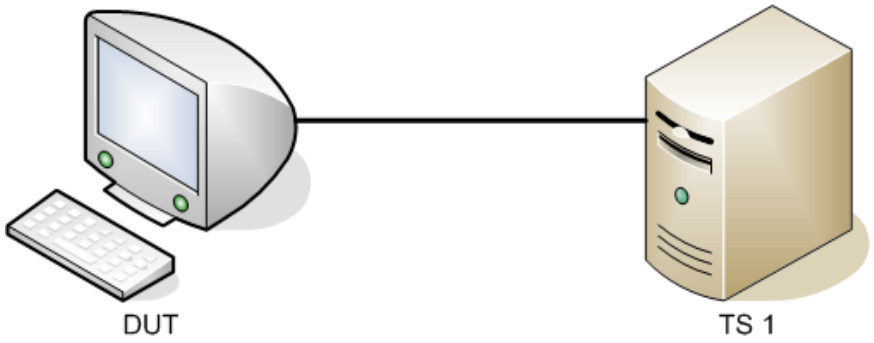
Resource Requirements:

- 1 Test Station

Discussion:

An EAP Response frame of type MD5 is sent when the Supplicant receives a request for credentials using the MD5-Challenge hash algorithm. The encoded credentials are sent within the response frame from the Supplicant to the Authenticator. The Authenticator then relays them to the Authentication Server which compares the MD5-Challenge hash to its stored credentials.

Test Layout:



Procedure:

Part A: EAPOL EAP Response MD5-Challenge

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl on the DUT to "Enable".
3. Start capture on Test Station 1.
4. Transmit a RequestForMD5Authentication frame from Test Station 1.
5. Stop capture on Test Station 1 and observe the captured frames (if any).

Observable Results:

- Test Station 1 must capture at least one EAPOL EAP Response frame. This frame must contain the following parameter values:

Destination Address:	0x0180C2000003
Source Address:	0x001234567890 (Must be equal to the MAC Address assigned to the DUT)
PAE Ethernet Type:	0x888E
Protocol Version:	0x01
Packet Type:	0x00
Packet Body Length:	0x0016
EAP Code:	0x02
EAP Identifier:	0x01
EAP Length:	0x0016
EAP Type:	0x04
EAP Value-Size:	0x10
EAP Value:	0x00112233445566778899AABBCCDDEEFF (This will be a unique field)

  To verify the EAP Value field, the value captured should be compared to a known MD5 hash of the RequestForMD5Authentication frame that is transmitted to the DUT.

Possible Problems:

- None

802.1X-Supp.op.3.6: EAPOL EAP Success Frame Validation

Purpose: This test verifies that an EAPOL EAP Success frame is properly interpreted.

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

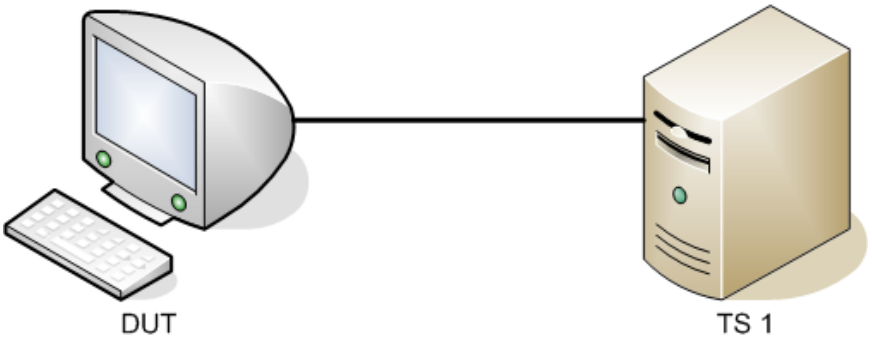
Resource Requirements:

- 1 Test Station

Discussion:

The EAP Success packet is sent from the Authenticator to the Supplicant. It informs the Supplicant that it has successfully authenticated with the 802.1X system. The Supplicant will now have complete access to the resources located on the LAN.

Test Layout:



Procedure:

Part A: EAPOL EAP Success

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl on the DUT to "Enabled".
3. Transmit a SupplicantAuthorized frame from Test Station 1.

Observable Results:

- In step 3, the current state of the DUT should be observed as "AUTHENTICATED" via management.

Possible Problems:

- None.

802.1X-Supp.op.3.7: EAPOL EAP Failure Frame Validation

Purpose: This test verifies that an EAPOL EAP Failure frame is properly interpreted.

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

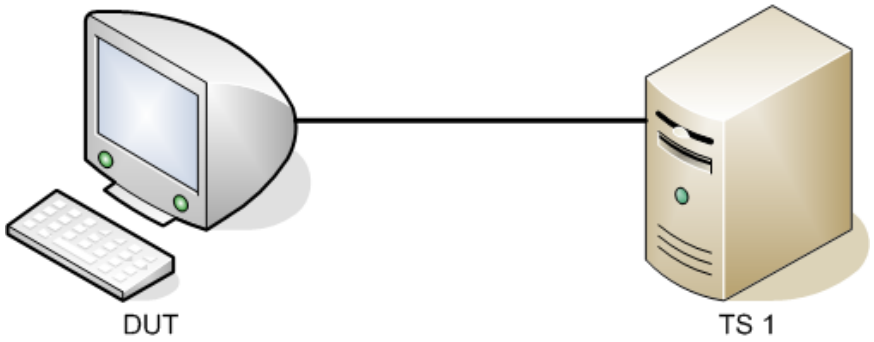
Resource Requirements:

- 1 Test Station

Discussion:

The EAP Failure packet is sent from the Authenticator to the Supplicant. It informs the Supplicant that it has failed authentication with the 802.1X system. The Supplicant will be put into the HELD state and will have to wait for heldWhile timer to expire. It can also make a new attempt at authentication if the Authenticator sends the Supplicant a request for its Identity.

Test Layout:



Procedure:

Part A: EAPOL EAP Failure

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl on the DUT to "Enabled".
3. Transmit a SupplicantFailure frame from Test Station 1.

Observable Results:

- In step 3, the current state of the DUT should be observed as "HELD" via management.

Possible Problems:

- None.

GROUP 4: Supplicant PAE State Machine

Scope

This group tests the different states and transitions into those states of the Supplicant PAE State Machine as described in IEEE Std 802.1X-2001: sub-clause 8.5.

Overview

- Logoff to Disconnected to Connecting
- Disconnected to Connecting
- Held to Connecting
- Held to Restart
- Connecting to Connecting
- Connecting to Restart
- Connecting to Authenticated
- Restart to Authenticating
- Authenticating to Held
- Authenticating to Connecting
- Authenticating to Authenticated
- Authenticated to Restart

802.1X-Supp.op.4.1 : Transition LOGOFF ⟶ DISCONNECTED ⟶ CONNECTING

Purpose: To ensure the DUT properly transitions from the LOGOFF state to the DISCONNECTED state; the DUT should then make the Unconditional Transition (UCT) to the CONNECTING state.

References:

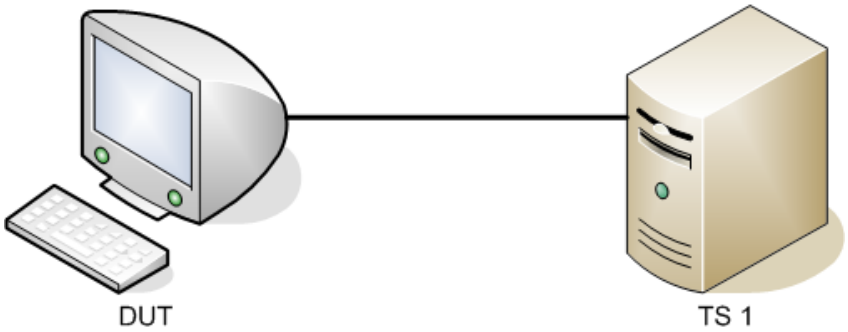
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11

Resource Requirements:

- 1 Test Station

Discussion: While in the LOGOFF state, if a user's Supplicant status is changed to Logged on, the Supplicant should transition to the DISCONNECTED state. The DUT should make an unconditional transition (UCT) to the CONNECTING state from the DISCONNECTED state. Once in the CONNECTING state an EAPOL-Start message is then transmitted from the DUT to the Authenticator.

Test Layout:



Procedure:

Part A: Transition LOGOFF to DISCONNECTED to CONNECTING

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl parameter on the DUT to "Enabled".
3. Start capture on Test Station 1.
4. Configure the userLogoff parameter on the DUT to true.
5. Stop capture on Test Station 1 and observe captured frames (if any).
6. Start capture on Test Station 1.
7. Disconnect or disable the link between the DUT and Test Station 1.
8. Configure the userLogoff parameter on the DUT to false.
9. Connect or enable the link between the DUT and Test Station 1.
10. Stop capture on Test Station 1 and observe captured frames (if any).

Part B: Transition LOGOFF to DISCONNECTED to CONNECTING (UCT)

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl parameter on the DUT to "Enabled".
3. Start capture on Test Station 1.
4. Configure the userLogoff parameter on the DUT to true.
5. Configure the userLogoff parameter on the DUT to false.
6. Stop capture on Test Station 1 and observe captured frames (if any).

Observable Results:

Part A:

- In step 4, the current state of the DUT should be observed via management as "LOGOFF".
- In step 5, Test Station 1 should receive one EAPOL-Logoff frame.
- In step 8, the current state of the DUT should be observed via management as "DISCONNECTED".
- In step 10, the current state of the DUT should be observed via management as "CONNECTING".
- In step 10, Test Station 1 should receive one EAPOL-Start frame.
- In step 4 and step 10, the DUT's suppStatus should be Unauthorized.

Part B:

- In step 4, the current state of the DUT should be observed via management as "DISCONNECTED".
- In step 4, the DUT's suppStatus should be Unauthorized.
- In step 6, Test Station 1 should receive one EAPOL-Logoff frame and one EAPOL-Start frame.
- In step 6, the current state of the DUT should be observed via management as "CONNECTING".

Possible Problems:

- If the DUT does not support configuration of the userLogoff variable, this test cannot be completed.

802.1X-Supp.op.4.2 : Transition DISCONNECTED ⟶ CONNECTING

Purpose: To ensure the DUT properly transitions from the DISCONNECTED state to the CONNECTING state, upon a UCT (Unconditional Transition).

References:

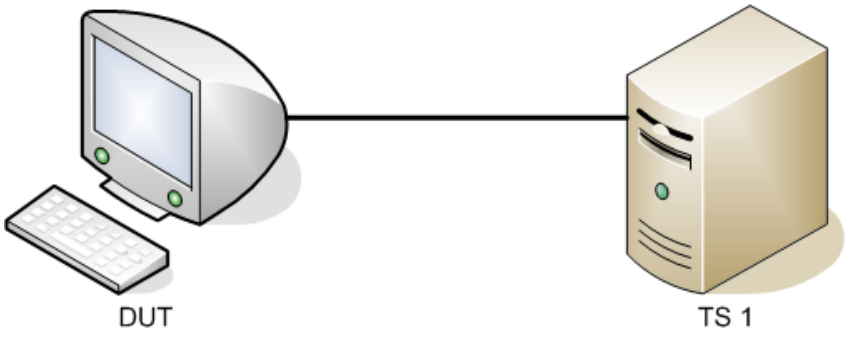
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11

Resource Requirements:

- 1 Test Station

Discussion: While in the DISCONNECTED state, a device should not receive an EAP Success or an EAP Failure frame from the Authenticator. A device within the DISCONNECTED state also should not transmit an EAPOL-Logoff Message directed to the Authenticator. A device within the DISCONNECTED state should make an unconditional transition (UCT) to the CONNECTING state, where up the device (Supplicant) should transmit an EAPOL-Start Message to the Authenticator.

Test Layout:



Procedure:

Part A: Transition DISCONNECTED to CONNECTING

1. Ensure that the default values are configured on the DUT.
2. Disconnect or disable the link between the DUT and Test Station 1.
3. Start capture on Test Station 1.
4. Set the SystemAuthControl parameter on the DUT to "Enabled".
5. Connect or enable the link between the DUT and Test Station 1.
6. Stop capture on Test Station 1.

Observable Results:

- In step 4, the current state of the DUT should be observed via management as "DISCONNECTED".
- In step 6, the current state of the DUT should be observed via management as "CONNECTING".
- In step 6, Test Station 1 should receive one EAPOL-Start frame.

Possible Problems:

- None.

802.1X-Supp.op.4.3 : Transition HELD ⟶ CONNECTING

Purpose: To ensure the DUT's Supplicant PAE state machine properly transitions from the HELD state to the CONNECTING state.

References:

- IEEE Std. 802.1X-2004: sub-clause 8.2.2.1
- IEEE Std. 802.1X-2004: sub-clause 8.2.3
- IEEE Std. 802.1X-2004: sub-clause 8.2.11
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.4
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.7
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.1.2
- IEEE Std. 802.1X-2004: Figure 8-9
- IEEE Std. 802.1X-2004: Figure 8-17

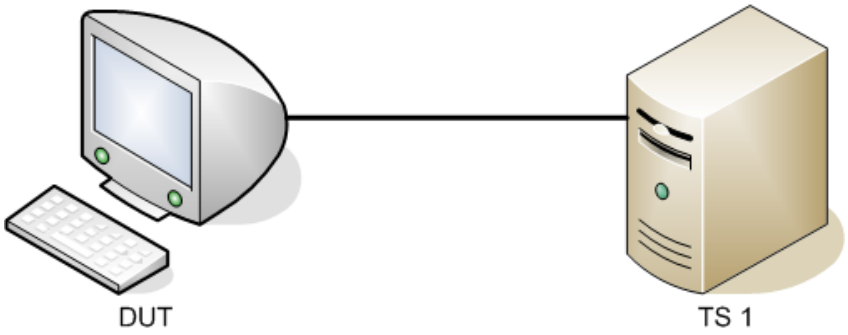
Resource Requirements:

- 1 Test Station

Discussion:

When the Supplicant PAE state machine enters the HELD state, the *heldWhile* timer is initialized with a value equal to the currently configured *heldPeriod* parameter value (default *heldPeriod* value = 60 seconds). The *heldWhile* timer is then decremented every second by the Port Timers state machine. If *reqId* is not asserted prior to expiry of the *heldWhile* timer, then the DUT's Supplicant PAE state machine must transition to the CONNECTING state when the *heldWhile* timer expires.

Test Layout:



Procedure:

Part A: Transition HELD to CONNECTING

1. Ensure that the default values are configured on the DUT.
2. Configure the SystemAuthControl parameter on the DUT to "Enabled".
3. Transmit a SupplicantFailure frame from Test Station 1.
4. Begin capture on Test Station 1.
5. Wait 62 seconds.
6. Stop capture on Test Station 1.

Observable Results:

- In step 4, the current state of the DUT should be observed via management as "HELD".
- In step 6, the current state of the DUT should be observed via management as "CONNECTING".
- In step 6, Test Station 1 must receive one properly formatted EAPOL-Start frame.
- In step 6, the DUT's suppStatus should remain Unauthorized.

Possible Problems:

- None.

802.1X-Supp.op.4.4 : Transition HELD ⟶ RESTART

Purpose: To ensure the DUT properly transitions from the HELD state to the RESTART state, upon reception of an EAPOL EAP Request/Identity frame from the Authenticator.

References:

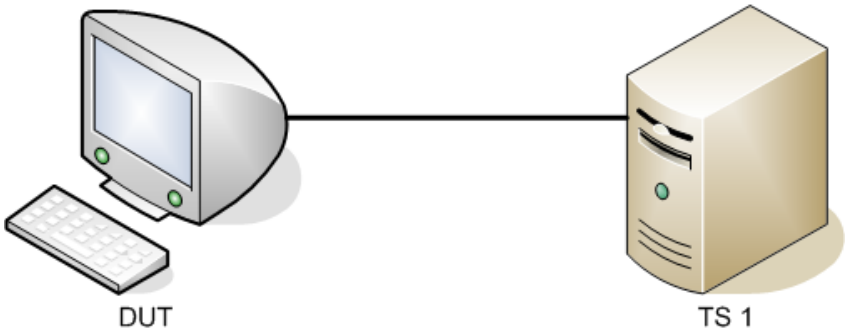
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.6

Resource Requirements:

- 1 Test Station

Discussion: While in the HELD state, a device should not receive from the authenticator an EAPOL EAP Success frame or an EAPOL EAP Failure frame. Within the HELD state, a device should set the heldWhile value equal to heldPeriod, which is set by default to 60 s. Upon reception of an EAPOL EAP Request/Identity frame from the Authenticator, the DUT should transition to the RESTART state. After transitioning, the Supplicant should transmit an EAPOL EAP Response/Identity frame to the Authenticator.

Test Layout:



Procedure:

Part A: Transition HELD to RESTART

1. Ensure the default values are configured on the DUT.
2. Configure the SystemAuthControl parameter on the DUT to "Enabled".
3. Transmit a SupplicantFailure frame from Test Station 1.
4. Begin capture on Test Station 1.
5. Within 10 seconds transmit a RequestSupplicantIdentity frame from Test Station 1.
6. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
7. Stop capture on Test Station 1 and observe the captured frames (if any).

Observable Results:

- In step 4, the current state of the DUT should be observed via management as "HELD".
- In step 6, the current state of the DUT should be observed via management as "RESTART".
- In step 6, Test Station 1 should receive one EAPOL-EAP-Response/Identity frame.

Possible Problems:

- None.

802.1X-Supp.op.4.5 : Transition CONNECTING ⟶ CONNECTING

Purpose: To ensure the DUT properly stays within the CONNECTING state when the startWhen timer expires.

References:

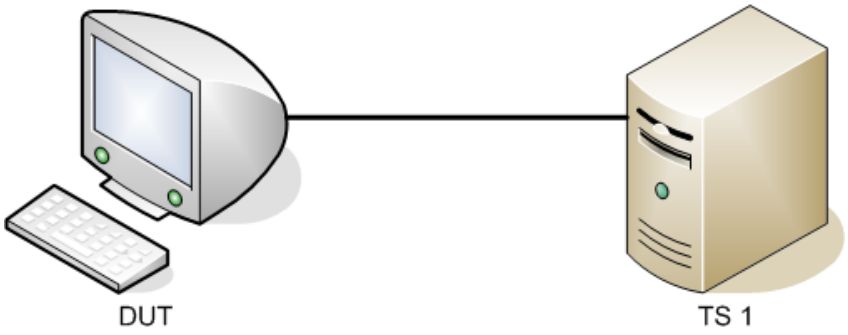
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.4

Resource Requirements:

- 1 Test Station

Discussion: While in the CONNECTING state, a device should transmit an EAPOL-Start frame directed to the Authenticator as well as not receive an EAPOL EAP Request/Identity frame from the Authenticator. When the Supplicant startWhen timer expires (startWhen ==0) and the Supplicant has not transmitted 3 successive EAPOL Start frames, the DUT should transition back into the CONNECTING state. After transitioning, the Supplicant's startWhen timer should be initialized to 30 seconds.

Test Layout:



Procedure:

Part A: Transition CONNECTING to CONNECTING

1. Ensure the default values are configured on the DUT.
2. Configure the SystemAuthControl on the DUT to "Enable".
3. Verify the DUT is in the CONNECTING state via management.
4. Start capture on Test Station 1.
5. Wait 30 seconds.
6. Stop capture on Test Station 1 and observe the captured frames (if any).

Observable Results:

- In step 6, the current state of the DUT should be observed via management as "CONNECTING".
- In step 6, Test Station 1 should receive one EAPOL Start frame.

Possible Problems:

- None.

802.1X-Supp.op.4.6 : Transition CONNECTING ⟶ RESTART

Purpose: To ensure the DUT properly transitions from the CONNECTING state to the RESTART state, upon reception of an EAPOL EAP Request/Identity packet from the Authenticator.

References:

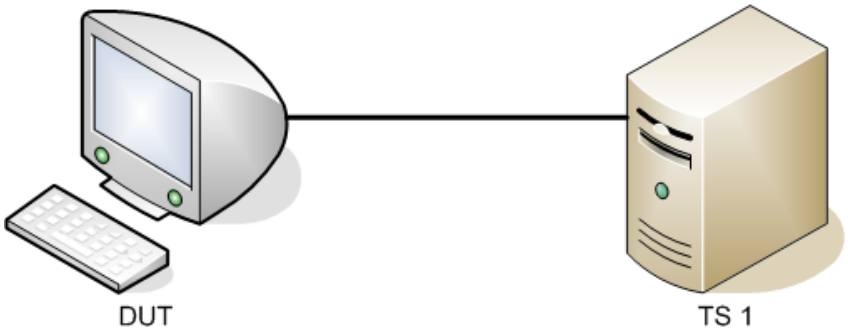
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.4

Resource Requirements:

- 1 Test Station

Discussion: While in the CONNECTING state, a device should transmit an EAPOL Start Message directed to the Authenticator as well as not receive an EAPOL EAP Request/Identity frame from the Authenticator. Upon reception of an EAPOL EAP Request/Identity frame from the Authenticator, the DUT should transition to the RESTART state. After transitioning, the Supplicant should transmit an EAPOL EAP Response/Identity frame to the Authenticator.

Test Layout:



Procedure:

Part A: Transition – CONNECTING to RESTART

1. Ensure that the default values are configured on the DUT.
2. Configure the SystemAuthControl parameter on the DUT to "Enabled".
3. Verify the DUT is in the CONNECTING state via management.
4. Start capture on Test Station 1.
5. Within 30 seconds transmit a RequestSupplicantIdentity frame from Test Station 1.
6. If prompted by the DUT, enter the Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
7. Stop capture on Test Station 1 and observe the captured frames (if any).

Observable Results:

- In step 7, the current state of the DUT should be observed via management as "RESTART".
- In step 7, Test Station 1 should receive one EAPOL-EAP-Response/Identity frame.

Possible Problems:

- None.

802.1X-Supp.op.4.7 : Transition CONNECTING ⟶ AUTHENTICATED

Purpose: To ensure the DUT properly transitions from the CONNECTING state to the AUTHENTICATED state.

References:

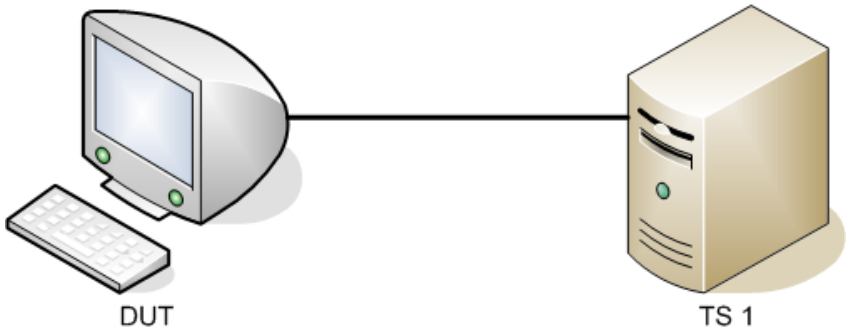
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.4

Resource Requirements:

- 1 Test Station

Discussion: While in the CONNECTING state, a device should transmit an EAPOL Start frame directed to the Authenticator as well as not receive an EAPOL EAP Request/Identity frame from the Authenticator. When the Supplicant does not receive responses from the Authenticator after transmitting 3 successive EAPOL Start frames and the startWhen counter==0, the DUT should transition to the AUTHENTICATED state. After transitioning, the Supplicant status (suppStatus) should be set to Authorized.

Test Layout:



Procedure:

Part A: Transition CONNECTING to AUTHENTICATED

1. Ensure that the default values are configured on the DUT.
2. Configure the SystemAuthControl parameter on the DUT to "Enable".
3. Start capture on Test Station 1.
4. Verify the DUT is in the CONNECTING state via management.
5. Wait 92 seconds.
6. Stop capture on Test Station 1 and observe captured frames (if any).

Observable Results:

- In step 6, Test Station 1 should receive 3 EAPOL-Start frames, at a rate of 1 EAPOL frame per 30 seconds.
- In step 6, the current state of the DUT should be observed via management as "AUTHENTICATED".

Possible Problems:

- None.

802.1X-Supp.op.4.8 : Transition RESTART ⟶ AUTHENTICATING

Purpose: To ensure the DUT properly transitions from the RSETART state to the AUTHENTICATING state, Upon completion of the eapRestart assertion.

References:

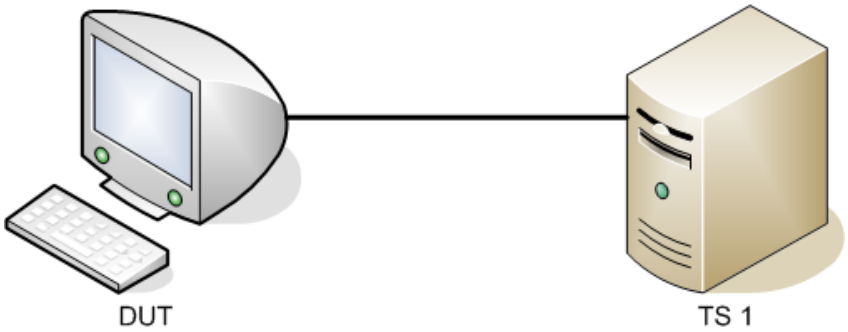
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.8

Resource Requirements:

- 1 Test Station

Discussion: While in the RESTART state, a device should set the eapRestart variable to TRUE. When the DUT's higher layer has acknowledged the Supplicant PAE restart and reset the eapRestart variable to FALSE, it should transition to the AUTHENTICATING state.

Test Layout:



Procedure:

Part A: Transition RESTART to AUTHENTICATING

1. Ensure that the default values are configured on the DUT.
2. Configure the SystemAuthControl parameter on the DUT to "Enable".
3. Transmit a RequestSupplicantIdentity frame from Test Station 1.
4. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
5. Verify the DUT is in the RESTART state via management.
6. Begin capture on Test Station 1.
7. Within 30 seconds transmit a RequestForMD5Authentication frame from Test Station 1.
8. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
9. Stop capture on Test Station 1 and observe captured frames (if any).

Observable Results:

- In step 9, the current state of the DUT should be observed via management as "AUTHENTICATING".
- In step 9, Test Station 1 should capture one EAPOL EAP Response frame.

Possible Problems:

- None

802.1X-Supp.op.4.9 : Transition AUTHENTICATING ⟶ HELD

Purpose: To ensure the DUT properly transitions from the AUTHENTICATING state to the HELD state, upon reception of an EAPOL EAP Failure frame from the Authenticator.

References:

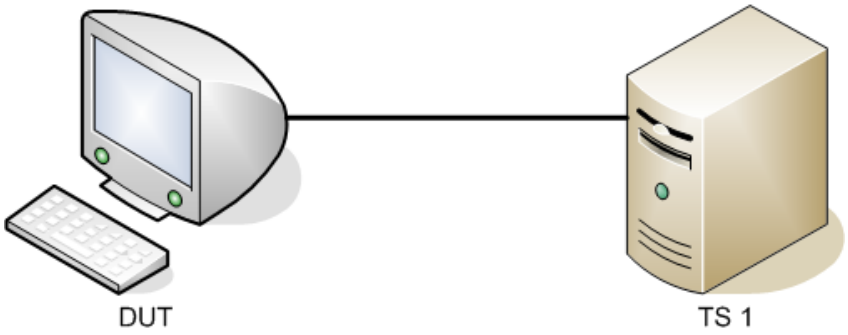
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.5

Resource Requirements:

- 1 Test Station

Discussion: While in the AUTHENTICATING state, a device should transmit to the Authenticator an EAPOL frame containing an EAP-Response other than an EAP-Response/Identity. A device within the AUTHENTICATING state also set the authWhile timer. When the DUT receives an EAPOL frame of type EAP Failure, it should transition to the RESTART state.

Test Layout:



Procedure:

Part A: Transition AUTHENTICATING to RESTART

1. Ensure that the default values are configured on the DUT.
2. Configure the SystemAuthControl parameter on the DUT to "Enable".
3. Transmit a RequestSupplicantIdentity frame from Test Station 1.
4. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
5. Within 30 seconds transmit a RequestForMD5Authentication frame from Test Station 1.
6. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
7. Begin capture on Test Station 1.
8. Verify the DUT is in the AUTHENTICATING state via management.
9. Within 30 seconds transmit a SupplicantFailure frame from Test Station 1.
10. Stop capture on Test Station 1 and observe captured frames (if any).

Observable Results:

- In step 10, the current state of the DUT should be observed via management as "RESTART".
- In step 10, Test Station 1 should capture one EAPOL-EAP-Response/Identity frame.

Possible Problems:

- None.

802.1X-Supp.op.4.10 : Transition AUTHENTICATING ⟶ CONNECTING

Purpose: To ensure the DUT properly transitions from the AUTHENTICATING state to the CONNECTING state.

References:

- IEEE Std. 802.1X-2001: sub-clause 8.2.2
- IEEE Std. 802.1X-2001: sub-clause 8.2.11.1.2
- IEEE Std. 802.1X-2001: sub-clause 8.2.11.4
- IEEE Std. 802.1X-2001: sub-clause 8.2.11.5

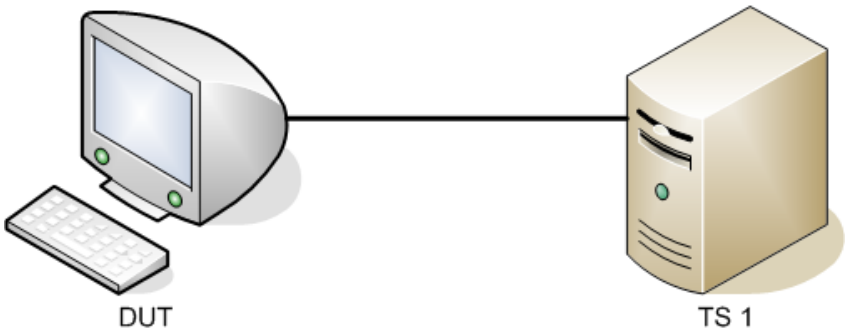
Resource Requirements:

- 1 Test Station

Discussion:

When the Supplicant PAE State Machine reaches the AUTHENTICATING state, the Supplicant transmits an EAPOL EAP Response frame, and waits for a response. At the time the EAPOL EAP Response frame is sent, the Supplicant sets the authWhile timer to the value contained in the authPeriod constant. Upon expiry of the authWhile timer, the Supplicant PAE State Machine transitions to the CONNECTING state.

Test Layout:



Procedure:

Part A: AUTHENTICATING to CONNECTING Transition

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl parameter on the DUT to "Enabled".
3. Transmit a RequestSupplicantIdentity frame from Test Station 1.
4. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
5. Transmit a RequestForMD5Authentication frame from Test Station 1.
6. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
7. Start capture on Test Station 1.
8. Verify the DUT is in the AUTHENTICATING state via management.
9. Wait 32 seconds.
10. Stop capture on Test Station 1 and observe captured frames (if any).

Observable Results:

- In step 10, the current state of the DUT should be observed via management as "CONNECTING".
- In step 10, Test Station 1 should receive one EAPOL-Start frame.

Possible Problems:

- None.

802.1X-Supp.op.4.11: Transition AUTHENTICATING ⟶ AUTHENTICATED

Purpose: To ensure the DUT properly transitions from the AUTHENTICATING state to the AUTHENTICATED state, upon reception of an EAPOL EAP Success frame from the Authenticator.

References:

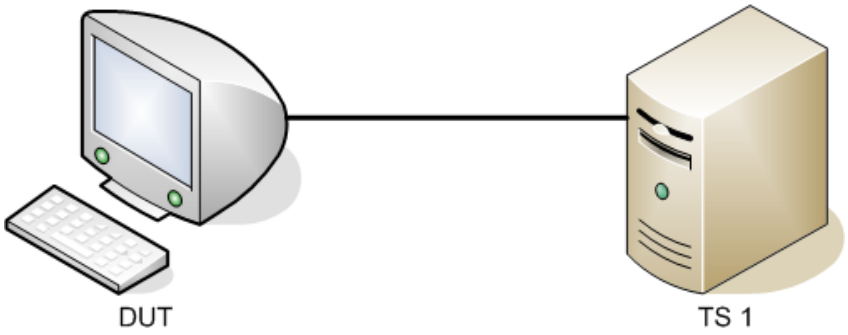
- IEEE Std. 802.1X-2004: sub-clause 8.2.2
- IEEE Std. 802.1X-2004: sub-clause 8.2.11.5

Resource Requirements:

- 1 Test Station

Discussion: While in the AUTHENTICATING state, a device should transmit to the Authenticator an EAPOL frame containing an EAP-Response other than an EAP-Response/Identity. A device within the AUTHENTICATING state also set the authWhile timer. When the DUT receives an EAPOL frame of type EAP Success, it should transition to the AUTHENTICATED state.

Test Layout:



Procedure:

Part A: Transition AUTHENTICATING to AUTHENTICATED

11. Ensure that the default values are configured on the DUT.
12. Configure the SystemAuthControl parameter on the DUT to "Enable".
13. Transmit a RequestSupplicantIdentity frame from Test Station 1.
14. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
15. Within 30 seconds transmit a RequestForMD5Authentication frame from Test Station 1.
16. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
17. Begin capture on Test Station 1.
18. Verify the DUT is in the AUTHENTICATING state via management.
19. Within 30 seconds transmit a SupplicantSuccess frame from Test Station 1.
20. Stop capture on Test Station 1 and observe captured frames (if any).

Observable Results:

- In step 10, the current state of the DUT should be observed via management as "AUTHENTICATED".

Possible Problems:

- None.

802.1X-Supp.op.4.12: Transition AUTHENTICATED ⟶ RESTART

Purpose: To ensure the DUT properly transitions from the AUTHENTICATED state to the RESTART state, upon reception of an EAPOL EAP Request/Identity frame from the Authenticator.

References:

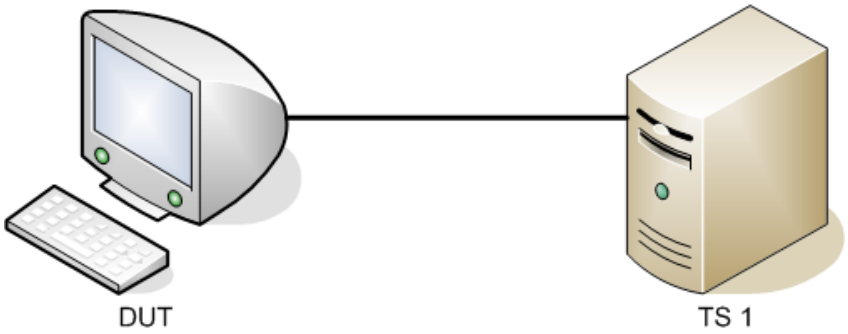
- IEEE Std. 802.1X-2001: sub-clause 8.2.2
- IEEE Std. 802.1X-2001: sub-clause 8.2.11.7

Resource Requirements:

- 1 Test Station

Discussion: While in the AUTHENTICATED state, a device should not receive from the authenticator an EAPOL EAP Success frame or an EAPOL EAP Failure frame. When the DUT receives an EAPOL frame of type EAP Request/Identity, it should transition to the RESTART state.

Test Layout:



Procedure:

Part A: Transition AUTHENTICATED to RESTART

1. Ensure that the default values are configured on the DUT.
2. Set the SystemAuthControl parameter on the DUT to "Enabled".
3. Transmit a SupplicantAuthorized frame from Test Station 1.
4. Start capture on Test Station 1.
5. Verify the DUT is in the AUTHENTICATED state via management.
6. Transmit a RequestSupplicantIdentity frame from Test Station 1.
7. If prompted by the DUT, enter a Username and Password of "good" and "ioltemp" respectively and submit the credentials on the DUT.
8. Stop capture on Test Station 1 and observe captured frames (if any).

Observable Results:

- In step 7, the current state of the DUT should be observed via management as "RESTART".
- In step 7, Test Station 1 should capture one EAPOL-EAP-Response/Identity frame.

Possible Problems:

- None

ANNEX A: Frame Descriptions

Scope

This Annex will describe all of the frames sent to the DUT within this Test Suite.

Overview

This will define the following frames:

- RequestSupplicantIdentity
- RequestForUnknownMechanism
- RequestForMD5Authenticaiton
- SupplicantAuthorized
- SupplicantFailure

802.1X-Supp.op.A.1 : RequestSupplicantIdentity Frame

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

Frame Format:

EAPOL Fields	Destination Address:	01 80 C2 00 00 03
	Source Address:	00 00 00 00 BF C1
	PAE Ethernet Type:	88 8E
	Protocol Version:	01
	Packet Type:	00 (EAP)
	Packet Body Length:	00 05
EAP Fields	EAP Code:	01 (Request)
	EAP Identifier:	01
	EAP Length:	00 05
	EAP Type:	01 (Identity)

802.1X-Supp.op.A.2 : RequestForUnknownMechanism Frame

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

Frame Format:

EAPOL Fields	Destination Address:	01 80 C2 00 00 03
	Source Address:	00 00 00 00 BF C1
	PAE Ethernet Type:	88 8E
	Protocol Version:	01
	Packet Type:	00 (EAP)
	Packet Body Length:	00 05
EAP Fields	EAP Code:	01 (Request)
	EAP Identifier:	01
	EAP Length:	00 05
	EAP Type:	0A (Unknown Authentication Method)

802.1X-Supp.op.A.3 : RequestForMD5Authentication Frame

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

Frame Format:

EAPOL Fields	Destination Address:	01 80 C2 00 00 03
	Source Address:	00 00 00 00 BF C1
	PAE Ethernet Type:	88 8E
	Protocol Version:	01
	Packet Type:	00 (EAP)
	Packet Body Length:	00 16
EAP Fields	EAP Code:	01 (Request)
	EAP Identifier:	01
	EAP Length:	00 16
	EAP Type:	04 (MD5-Challenge)
	EAP Value-Size:	10
	EAP Value:	00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF

802.1X-Supp.op.A.4 : SupplicantAuthorized Frame

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

Frame Format:

EAPOL Fields	Destination Address:	01 80 C2 00 00 03
	Source Address:	00 00 00 00 BF C1
	PAE Ethernet Type:	88 8E
	Protocol Version:	01
	Packet Type:	00 (EAP)
	Packet Body Length:	00 04
EAP Fields	EAP Code:	03 (Success)
	EAP Identifier:	01
	EAP Length:	00 04

802.1X-Supp.op.A.5 : SupplicantFailure Frame

References:

- IEEE Std. 802.1X-2004: sub-clause 7.1
- IEEE Std. 802.1X-2004: sub-clause 7.2
- IEEE Std. 802.1X-2004: sub-clause 7.5
- IEEE Std. 802.1X-2004: sub-clause 7.7
- IETF RFC 2284 – EAP

Frame Format:

EAPOL Fields	Destination Address:	01 80 C2 00 00 03
	Source Address:	00 00 00 00 BF C1
	PAE Ethernet Type:	88 8E
	Protocol Version:	01
	Packet Type:	00 (EAP)
	Packet Body Length:	00 04
EAP Fields	EAP Code:	04 (Failure)
	EAP Identifier:	01
	EAP Length:	00 04