Wireless LAN Consortium

802.11 WPA2 Access Point MAC Conformance Test Suite v2.4 Report

UNH InterOperability Laboratory — 121 Technology Drive, Suite 2 — Durham, NH 03824 — +1-603-862-2263

January 3, 2013
Report Rev. 1.0

Joe Vendor
Magic Wireless Company
52 OFDM Drive
Mimo, NH 010111

Mr. Vendor,

Enclosed are the results from the Wireless WPA2 Access Point MAC Conformance Test Suite testing performed on the:

Magic Device Name MD-360 802.11a/b/g Access Point

This testing pertains to a set of standard requirements, put forth in the IEEE Std 802.11-2007 Edition. The tests performed are part of the 802.11 WPA2 AP MAC Conformance Test Suite v2.4, which is available on the UNH-IOL's website:

ftp://ftp.iol.unh.edu/pub/wireless/TestSuites/mac/802.11_AP_WPA2_MAC_Conformance_Test_Suite_v2.4.pdf

Issues Observed While Testing
1.3.2: Key Information Field Processing: Part a - The DUT was observed to incorrectly discard an EAPoL-Key Message 2 containing reserved bits in Key Information Field.
1.3.2: Key Information Field Processing: Part c - The DUT was observed to not discard an EAPoL-Key Message 4 frame containing the error bit set.
1.3.3: Key Length Field Processing: Part a - The DUT was observed to incorrectly process an EAPoL-Key Message 2 containing a Key Length value of 32.
1.3.3: Key Length Field Processing: Part b - The DUT was observed to incorrectly process an EAPoL-Key Message 4 containing a Key Length value of 32.
1.3.5: Key Nonce Field Processing: Part b - The DUT was observed to incorrectly complete the 4-way handshake upon reception of an EAPoL-Key Message 4 frame containing a non-zero Key Nonce.

As always, we welcome any comments regarding this Test Suite. If you have any questions about the test procedures or results, please contact me via e-mail at TJ.Tester@iol.unh.edu or by phone at +1-603-862-2263.

Regards,

TJ MCTester

UNH-IOL
2013.01.03 16:15:24 -05'00'

DIGITAL SIGNATURE INFORMATION

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

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

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

MD5 Fingerprint: **EEE1 7A82 7806 EB21 AF94 F189 E4BE 361B**
SHA-1 Fingerprint: **ECFB 7FAF AB4A 0832 2408 E965 9F5C E3F2 D784 AAAB**

Table 1 - Result Key - The following table contains possible results and their meanings

Result	Interpretation
PASS	The DUT was observed to exhibit conformant behavior.
FAIL	The DUT was observed to exhibit non-compliant behavior.
PASS with Comments	The DUT was observed to exhibit conformant behavior, however, additional explanation of the situation is included.
Warning	The DUT was observed to exhibit behavior that is not recommended.
Informative	Results are for informative purposes only and are not judged on a pass or fail basis.
Refer to Comments	From the observations, a valid pass or fail could not be determined. An additional explanation of the situation is included.
Not Applicable	The DUT does not support the technology required to perform these tests.
Not Available	Due to testing station or time limitations, the tests could not be performed, or were performed in a limited capacity.
Not Tested	Not tested due to time constraint of the test period.
Borderline	The observed values of the specified parameter are valid at one extreme, and invalid at the other.

Table 2 - Setup and Configuration Information

Product	
Manufacturer	Magic Device Machine
Model	MD-360
Hardware Version	3AGE3584
Firmware Version	8.4.2453
MAC Address	00:0M:0A:0C:00:00
Serial Number	FTH25489FE
IOL Label	VN-DUTT-00000123456
PSK	wireless
Test System Hardware	
RF Isolated Environment	USC-26 RF/EMI Isolation Chamber 16'x 8' x 8' @ 100dB
Sniffer	AiroPeek Sniffer (Proxim ORiNOCO 802.11 a/b/g/ card)
Test Station	Atheros DK4 Testing Station

SAMPLE REPORT

In many traces, identification frames were used to simplify result collecting. These frames are identified by their source MAC address (00:00:01:ba:bb:1e). Below is an example of an identification frame found in a trace:

No.	Info	Protocol	Source	Destination
1	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	Xerox_00:00:11	Broadcast
2	Part a: Non-Acknowledged Frames	Babble Frame	0.0.0.0	255.255.255.255
3	MSDU1 => ICMP Echo Request with Protocol Version > 0	Babble Frame	0.0.0.0	255.255.255.255
4	Echo (ping) request	ICMP	192.168.0.102	aa:bb:cc:dd:ee
5	Acknowledgement	IEEE 802.11		Xerox_00:00:11
6	Clear-to-send	IEEE 802.11		aa:bb:cc:dd:ee
7	Data	IEEE 802.11	Xerox_00:00:11	aa:bb:cc:dd:ee

Rows highlighted in green are Management Frames.
Rows highlighted in blue are Control Frames.
Rows highlighted in white are Data Frames.
Rows highlighted in violet are ICMP Echo Requests/Responses

Fields or Frame excerpts highlighted in this reports are important and directly related to the issue being shown in the trace excerpt.

SAMPLE REPORT

GROUP 1: CCMP ENCAPSULATION

Test # and Label	Part(s)	Result(s)
1.1.1: CCMP MIC Verification	**a**	**PASS**
	b	**PASS**
	c	**PASS**
	d	**PASS**
	e	**PASS**

Comments on Test Procedure

Purpose: To verify that CCMP encrypted data frames transmitted by the DUT contain a properly constructed MIC.

In an RSN, the encrypted MPDU uses a MIC to validate whether the frame has been received unaltered. The MIC is a function of the Nonce, TK, AAD, and plaintext data. CCMP processing expands the original MPDU size by 16 octets, 8 octets for the CCMP Header field and 8 octets for the MIC field. The MIC is calculated using the AES algorithm with CBC-MAC. This differs from the encryption of plaintext that uses the Counter Mode instead. Once the MIC is calculated, it is appended to the MPDU payload and finally the appended MPDU is encrypted.

The DUT should:
a. properly compute the cipher text and MIC using the TK, AAD, Nonce, and MPDU payload.
b. calculate the MIC transmitted to a unicast receiver address with the PTK.
c. calculate the MIC transmitted to a group receiver address with the GTK.
d. should append the MIC to the MPDU payload with exactly 8 bytes after fragmentation occurs.
e. should append the MIC to the MPDU prior to its encryption.

Comments on Test Results

a.-e. There were no issues uncovered during the testing process.

Test # and Label	Part(s)	Result(s)
1.1.2: CCMP Header Format	**a**	**PASS**
	b	**PASS**
	c	**PASS**
	d	**PASS**

Comments on Test Procedure

Purpose: To verify that CCMP encrypted data frames transmitted from the DUT format the CCMP header properly.

In an RSN, the encrypted MPDU inserts an 8 octet CCMP header after the MAC header and before the encrypted payload. The CCMP header consists of the Key ID, ExtIV and PN values. The Extended IV bit is always set. The PN is a 48-bit number that is incremented for each MPDU transmitted by the DUT and should never be repeated while the same TK is being used. All other bits are reserved and should be ignored on reception.

The DUT should:
a. add exactly 8 bytes to the MPDU after fragmentation for the CCMP header.
b. set the Extended IV bit to 1.
c. set reserved bits b0 to b4 of the 4th octet and all bits of the 3rd octet in the CCMP header to 0.
d. increment the PN for every MPDU transmitted.

Comments on Test Results

a-d. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.1.3: CCMP Encryption Verification	**a**	**PASS**
	b	**PASS**
	c	**PASS**
	d	**PASS**

Comments on Test Procedure

Purpose: To verify that CCMP encryption on frames transmitted by the DUT is implemented properly.

CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following steps. The PN is incremented to obtain a fresh PN for each MPDU so that the PN never repeats for the same temporal key. Note that retransmitted MPDUs are not modified on retransmission. Using the fields in the MPDU header construct the AAD for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being masked to 0 when calculating the AAD. The CCM Nonce block is constructed from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2. The new PN and the key identifier are placed into the 8-octet CCMP header. Using the temporal key, AAD, nonce, and MPDU data the cipher text and MIC are computed. This step is known as CCM originator processing. The encrypted MPDU is formed by combining the original MPDU header, the CCMP header, the encrypted data and MIC, as described in [1].

The DUT should:
a. properly compute the cipher text MPDU payload.
b. encrypt data transmitted to a unicast receiver address with the PTK.
c. not use a Key ID of 0 with the GTK.
d. encrypt data transmitted to a group receiver address with the GTK.

Comments on Test Results

a-d. There were no issues uncovered during the testing process.

SAMPLE REPORT

GROUP 2: CCMP DECAPSULATION

Test # and Label	Part(s)	Result(s)
1.2.1: CCMP MIC Processing	**a**	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT correctly calculates the MIC when decrypting CCMP encrypted data.

In an RSN, the encrypted MPDU uses a MIC to validate whether the frame has been received unaltered. The MIC is a function of the Nonce, TK, AAD, and plaintext data. CCMP processing expands the original MPDU size by 16 octets, 8 octets for the CCMP Header field and 8 octets for the MIC field. The MIC is calculated using the AES algorithm with CBC-MAC. This differs from the encryption of plaintext that uses the Counter Mode instead. Once the MIC is calculated, it is appended to the MPDU payload and finally the appended MPDU is encrypted.

a. The DUT should discard received MPDUs with invalid MICs (MSDU1, MSDU2, MSDU4).

Comments on Test Results

a. There were no issues uncovered during the testing process.

Test # and Label	Part(s)	Result(s)
1.2.2: CCMP Header Processing	**a**	**PASS**
	b	**PASS**
	c	**Informative**
Comments on Test Procedure		

Purpose: To verify that the DUT processes the CCMP header properly on received CCMP encrypted data frames.

In an RSN, the encrypted MPDU inserts an 8 octet CCMP header after the MAC header and before the encrypted payload. The CCMP header consists of the Key ID, ExtIV and PN values. The Extended IV bit is always set. The PN is a 48-bit number that is incremented for each MPDU transmitted by the DUT and should never be repeated while the same TK is being used. All other bits are reserved and should be transmitted as 0.

The DUT should:
a. ignore reserved bits b0 to b4 of the 4th octet and all bits of the 3rd octet in the CCMP header.
b. discard any CCMP encrypted frame with the Extended IV bit set to 0.
c. may discard any frame containing an invalid Key ID.

Comments on Test Results

a-c. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.2.3: CCMP Decryption Verification	**a**	**PASS**
	b	**PASS**
	c	**PASS**

Comments on Test Procedure

Purpose: To verify that CCMP decryption on frames is implemented properly.

CCMP decrypts the payload of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps. The encrypted MPDU is parsed to construct the AAD and nonce values. The AAD is formed from the MPDU header of the encrypted MPDU. The Nonce value is constructed from the A2, PN, and Priority Octet fields. The MIC is extracted for use in the CCM integrity checking. The CCM recipient processing uses the temporal key, AAD, nonce, MIC, and MPDU cipher text data to recover the MPDU plaintext data as well as to check the integrity of the AAD and MPDU plaintext data. The received MPDU header and the MPDU plaintext data from the CCM recipient processing may be concatenated to form a plaintext MPDU. The decryption processing prevents replay of MPDUs by validating that the PN in the MPDU is greater than the replay counter maintained for the session.

The DUT should:
a. properly decrypt and forward the response to MSDU1-4.
b. not be able to decrypt the frame and not forward the response to MSDU5.
c. not be able to decrypt the frame and not forward the response to MSDU6-11.

Comments on Test Results

a-c. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.2.4: CCMP PN Processing	**a**	**PASS**
	b	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT properly implements the PN packet replay procedure.

To effect replay detection, the receiver extracts the PN from the CCMP Header. This PN value shall be a 48-bit monotonically incrementing non-negative integer, initialized to one when the TK is initialized or refreshed. The PN values sequentially number each MPDU. A separate set of PN replay counters for each PTKSA, GTKSA, and STSL shall exist, and be initialized to zero whenever the TK is reset for a peer.

A receiver shall discard an MSDU if the constituent MPDU PN values are not sequential. A receiver shall discard any MPDU that is received with a PN less than or equal to the replay counter, and then shall increment the value of dot11RSNAStatsCCMPReplays for the key.

The DUT should:
a. only update its PN replay counter for valid CCMP MPDUs (MSDU1, MSDU3, MSDU5).
b. use the PN from the received MPDU to detect replayed frames and discard MSDUs whose constituent MPDU PN values are not sequential (MSDU7, MSDU10, MSDU13, MSDU16).

Comments on Test Results

a-b. There were no issues uncovered during the testing process.

SAMPLE REPORT

GROUP 3: EAPOL-KEY RECEPTION

Test # and Label	Part(s)	Result(s)
1.3.1: Descriptor Type Processing	**a**	**PASS**
	b	**PASS**
Comments on Test Procedure		
Purpose: To verify that the DUT can properly process the Descriptor Type field present in EAPoL-key frames. The Descriptor Type Field is one octet in length, taken to represent an unsigned binary number. The value defines the type of the Key Descriptor, which in turn defines how the Descriptor Body is used and interpreted. For 802.11 the Descriptor Type is 2. The DUT should: a. successfully complete the 4-way handshake. b. silently discard invalid EAPoL-Key frames.		
Comments on Test Results		
a-b. There were no issues uncovered during the testing process.		

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.3.2: Key Information Field Processing	**a**	**FAIL**
	b	**PASS**
	c	**FAIL**

Comments on Test Procedure

Purpose: To verify that the DUT can properly process the Key Information field present in EAPoL-key frames.

The Key Information Field is 2 octets in length and specifies characteristics of the key. The Key Information Field is comprised of the following fields, Key Descriptor Version, Key Type, Reserved, Install, Key MIC, Secure, Error, Request, Encrypted Key Data, SMK Message, and another Reserved. The values that should be contained within each field of the Key Information Field are specified within [1].

The DUT should:
a. ignore Key Information field reserved bits and successfully complete the 4-way handshake.
b. silently discard all EAPoL-Key frames containing invalid Key Descriptor Version types.
c. silently discard all incorrectly formatted EAPoL-Key frames.

Comments on Test Results

a. The DUT was observed to improperly discard an EAPoL-Key Message 2 containing reserved bit 13 of the Key Information Field set and did not successfully complete the 4-way handshake. The DUT should ignore Key Information field reserved bits and successfully complete the 4-way handshake. See IEEE Standard 802.11-2007 Edition, subclause 8.5.2. Please refer to Table 3 for more information regarding this test case.
b. There were no issues uncovered during the testing process.
c. The DUT was observed to not discard an EAPoL-Key Message 4 frame containing the error bit set and improperly completed the 4-way handshake. The DUT should silently discard all incorrectly formatted EAPoL-Key frames. See IEEE Standard 802.11-2007 Edition, subclause 8.5.2. Please refer to Table 4 for more information regarding this test case.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.3.3: Key Length Field Processing	**a**	**FAIL**
	b	**FAIL**

Comments on Test Procedure

Purpose: To verify that the DUT can properly process the Key Length field present in EAPoL-key frames.

The Key Length Field is 2 octets in length, represented as an unsigned binary number. The value defines the length, in octets, of the PTK to configure into IEEE Std 802.11.

The DUT should:
a. silently discard all EAPoL-Key Message 2 frames with non-zero Key Lengths.
b. silently discard all EAPoL-Key Message 4 frames with non-zero Key Lengths.

Comments on Test Results

a. The DUT was observed to improperly process an EAPoL-Key Message 2 containing a Key Length value of 32. The DUT should silently discard all EAPoL-Key Message 2 frames with non-zero Key Lengths. See IEEE Standard 802.11-2007 Edition, subclause 8.5.2. Please refer to Table 5 for more information regarding this test case.
b. The DUT was observed to improperly process an EAPoL-Key Message 4 containing a Key Length value of 32. The DUT should silently discard all EAPoL-Key Message 4 frames with non-zero Key Lengths. See IEEE Standard 802.11-2007 Edition, subclause 8.5.2. Please refer to Table 6 for more information regarding this test case.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.3.4: Key Replay Counter Processing	**a**	**PASS**
	b	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT can properly process the Key Replay Counter field present in EAPoL-key frames.

The Key Replay Counter Field is 8 octets, represented as an unsigned binary number, and is initialized to 0 when the PMK is established. The Supplicant shall use the key replay counter in the received EAPOL-Key frame when responding to an EAPOL-Key frame. It carries a sequence number that the protocol uses to detect replayed EAPOL-Key frames. The Supplicant and Authenticator shall track the key replay counter per security association. The Key Replay Counter shall be initialized to 0 on (re)association. The Authenticator shall increment the key replay counter on each successive EAPOL-Key frame. When replying to a message from the Authenticator, the Supplicant shall use the Key Replay Counter field value from the last valid EAPOL-Key frames received from the Authenticator.

The Authenticator should use the key replay counter to identify invalid messages to silently discard. The Supplicant should also use the Key Replay Counter and ignore EAPOL-Key frames with a Key Replay Counter field value smaller than or equal to any received in a valid message. The local Key Replay Counter field should not be updated until the after EAPOL-Key MIC is checked and is valid. In other words, the Supplicant never updates the Key Replay Counter field for Message 1 in the 4-Way Handshake, as it includes no MIC. This implies the Supplicant must allow for retransmission of Message 1 when checking for the key replay counter of Message 3.

The DUT should:
a. silently discard EAPoL-Key Messages with invalid Key Replay Counter fields.
b. not successfully complete the 4-way handshake.

Comments on Test Results

a-b. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.3.5: Key Nonce Field Processing	**a**	**PASS**
	b	**FAIL**

Comments on Test Procedure

Purpose: To verify that the DUT can properly process the Key Nonce field present in EAPoL-key frames.

The Key Nonce Field is 32 octets. It conveys the ANonce from the Authenticator and the SNonce from the Supplicant. [1] states that the ANonce and SNonce shall be random or pseudo-random values that shall not repeat for any security association. Choosing the nonces randomly helps prevent precomputation attacks. With unpredictable nonces, a man-in- the-middle attack that uses the Supplicant to precompute messages to attack the Authenticator cannot progress beyond Message 2, and a similar attack against the Supplicant cannot progress beyond Message 3.

The DUT should:
a. receive MSDU1 without failure.
b. not successfully complete the 4-way handshake upon reception of MSDU2.

Comments on Test Results

a. There were no issues uncovered during the testing process.
b. The DUT was observed to improperly complete the 4-way handshake upon reception of an EAPoL-Key Message 4 frame containing a non-zero Key Nonce. The DUT should not successfully complete the 4-way handshake upon reception of an EAPoL-Key Message 4 frame with a non-zero Key Nonce. See IEEE 802.11-2007 Edition subclause 8.5.2 for more information regarding this test case. Please refer to Table 7 for more information regarding this test case.

Test # and Label	Part(s)	Result(s)
1.3.6: Key IV Field Processing	**a**	**FAIL**

Comments on Test Procedure

Purpose: To verify that the DUT can properly process the Key IV field present in EAPoL-key frames.

This field is 16 octets. It contains the IV used with the KEK. It shall contain 0 when an IV is not required. It should be initialized by taking the current value of the global key counter and then incrementing the counter. Note that only the lower 16 octets of the counter value will be used.

a. The DUT should silently discard all EAPoL-Key frames containing invalid EAPoL-Key IV fields.

Comments on Test Results

a. The DUT was observed to not discard an EAPoL-Key Message 2 containing a non-zero Key IV. The DUT should silently discard all EAPoL-Key frames containing invalid EAPoL-Key IV fields. See IEEE 802.11-2007 Edition subclause 8.5.2 for more information regarding this test case. Please refer to Table 8 for more information regarding this test case.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.3.7: Key RSC Field Processing	**a**	**FAIL**
Comments on Test Procedure		

Purpose: To verify that the DUT can properly process the Key RSC field present in EAPoL-key frames.

The Key RSC Field is 8 octets in length. It contains the RSC for the GTK being installed in IEEE Std 802.11. It is used in Message 3 of the 4-Way Handshake and Message 1 of the Group Key Handshake, where it is used to synchronize the IEEE 802.11 replay state. It may also be used in the Michael MIC Failure Report frame, to report the TSC field value of the frame experiencing a MIC failure. It shall contain 0 in other messages. The Key RSC field gives the current message number for the GTK, to allow a STA to identify replayed MPDUs. If the Key RSC field value is less than 8 octets in length, the remaining octets shall be set to 0. The least significant octet of the TSC or PN should be in the first octet of the Key RSC field.

a. The DUT should silently discard all EAPoL-Key frames containing invalid Key RSCs.

Comments on Test Results

a. The DUT was observed to not discard an EAPoL-Key Messsage containing a non-zero Key RSC. The DUT should silently discard all EAPoL-Key frames containing invalid Key RSCs. See IEEE 802.11-2007 Edition subclause 8.5.2 for more information regarding this test case. Please refer to Table 9 for more information regarding this test case.

Test # and Label	Part(s)	Result(s)
1.3.8: Reserved Octets Processing	**a**	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT can properly process the Reserved Octets 61-68 present in EAPoL-key frames of Descriptor Type 2.

[1] states that reserved bits should be set to 0 upon transmission and ignored upon reception.

a. The DUT should ignore reserved bits set within EAPoL-Key Messages.

Comments on Test Results

a. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.3.9: Key MIC Field Processing	**a**	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT can properly process the Key MIC field present in EAPoL-key frames.

The Key MIC Field is 16 octets in length when the Key Descriptor Version subfield is 1 or 2. The EAPOL-Key MIC is a MIC of the EAPOL-Key frames, from and including the EAPOL protocol version field to and including the Key Data field, calculated with the Key MIC field set to 0. If the Encrypted Key Data subfield (of the Key Information field) is set, the Key Data field is encrypted prior to computing the MIC.

a. The DUT should silently discard all EAPoL-Key frames with incorrect Key MIC fields.

Comments on Test Results

a. There were no issues uncovered during the testing process.

Test # and Label	Part(s)	Result(s)
1.3.10: Key Data Length Field Processing	**a**	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT can properly process the Key Data Length present in EAPoL-key frames.

The Key Data Length Field is 2 octets in length, taken to represent an unsigned binary number. This represents the length of the Key Data field in octets. If the Encrypted Key Data subfield (of the Key Information field) is set, the length is the length of the Key Data field after encryption, including any padding.

a. The DUT should receive EAPoL-Key frames with invalid Key Data Lengths without failure.

Comments on Test Results

a. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.3.11: Key Data Field Processing (Pairwise Message2)	**a**	**FAIL**
	b	**FAIL**
	c	**FAIL**

Comments on Test Procedure

Purpose: To verify that the DUT can properly process encrypted Key Data present in EAPoL-key frames of the 4-way handshake.

The Key Data Field is a variable-length field that is used to include any additional data required for the key exchange that is not included in the fields of the EAPOL-Key frame. The additional data may be zero or more information element(s) (such as the RSN information element) and zero or more key data cryptographic encapsulation(s) (KDEs) (such as GTK(s) or PMKID(s)). Information elements sent in the Key Data field include the Element ID and Length subfields. KDEs shall be encapsulated.

If the Encrypted Key Data subfield (of the Key Information field) is set, the entire Key Data field shall be encrypted. If the Key Data field uses the NIST AES key wrap, then the Key Data field shall be padded before encrypting if the key data length is less than 16 octets or if it is not a multiple of 8. The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received EAPOL-Key message, the receiver shall ignore this trailing padding. Key Data fields that are encrypted, but do not contain the GroupKey or SMK KDE, shall be accepted.

The DUT should:
a. ignore any IEs that are unknown (MSDU1).
b. ignore any pad bytes appended to an Encrypted Key Data field (MSDU2).
c. terminate the association if the RSN IE contained in the Key Data field does not bitwise match the RSN IE contained in the Association or Reassociation Request frame (MSDU3-6).

Comments on Test Results

a. The DUT was observed to incorrectly discard an EAPoL-Key Message 2 containing a reserved IE (EID 254). The DUT should ignore any IEs that are unknown or reserved and successfully complete the 4-way handshake. See IEEE 802.11-2007 Edition subclause 8.5.2 for more information regarding this test case. Please refer to Table 10 for more information regarding this test case.
b. The DUT was observed to incorrectly discard an EAPoL-Key Message 2 containing 7 octets of padding and a correct RSN IE. The DUT should ignore any pad bytes appended to an Encrypted Key Data field and successfully complete the 4-way handshake. See IEEE 802.11-2007 Edition subclause 8.5.2 for more information regarding this test case. Please refer to Table 11 for more information regarding this test case.
c. The DUT was observed to not transmit a Dissociation upon reception of an EAPoL-Key Message 2 containing a RSN IE different from association request RSN IE. The DUT should terminate the association if the RSN IE contained in the Key Data field does not bitwise match the RSN IE contained in the Association or Reassociation Request frame. See IEEE 802.11-2007 Edition subclause 8.5.2 for more information regarding this test case. Please refer to Table 12 for more information regarding this test case.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.3.12: Key Data Field Processing (Pairwise Message4)	**a**	**PASS**
	b	**PASS**
	c	**FAIL**

Comments on Test Procedure

Purpose: To verify that the DUT can properly process encrypted Key Data present in EAPoL-key frames of the 4-way handshake.

The Key Data Field is a variable-length field that is used to include any additional data required for the key exchange that is not included in the fields of the EAPOL-Key frame. The additional data may be zero or more information element(s) (such as the RSN information element) and zero or more key data cryptographic encapsulation(s) (KDEs) (such as GTK(s) or PMKID(s)). Information elements sent in the Key Data field include the Element ID and Length subfields. KDEs shall be encapsulated.

If the Encrypted Key Data subfield (of the Key Information field) is set, the entire Key Data field shall be encrypted. If the Key Data field uses the NIST AES key wrap, then the Key Data field shall be padded before encrypting if the key data length is less than 16 octets or if it is not a multiple of 8. The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received EAPOL-Key message, the receiver shall ignore this trailing padding. Key Data fields that are encrypted, but do not contain the GroupKey or SMK KDE, shall be accepted.

The DUT should:
a. accept EAPoL-Key frames with empty Key Data Fields.
b. receive MSDU2 without failure.
c. ignore any IEs or KDEs that are unknown.

Comments on Test Results

a-b. There were no issues uncovered during the testing process.
c. The DUT was observed to incorrectly discard an EAPoL-Key Message 4 containing Multiple Revered KDEs. The DUT should ignore any IEs or KDEs that are unknown and successfully complete the 4-way handshake. See IEEE 802.11-2007 Edition subclause 8.5.2 for more information regarding this test case. Please refer to Table 13 for more information regarding this test case.

SAMPLE REPORT

GROUP 4: EAPOL-KEY TRANSMISSION

Test # and Label	Part(s)	Result(s)
1.4.1: Descriptor Type Field Formatting	**a**	**PASS**

Comments on Test Procedure

Purpose: To verify that the DUT uses the proper Descriptor Type in EAPoL-key frames.

The Descriptor Type Field is one octet in length, taken to represent an unsigned binary number. The value defines the type of the Key Descriptor, which in turn defines how the Descriptor Body is used and interpreted. For 802.11 the Descriptor Type is 2.

a. The DUT should transmit EAPoL-Key frames with a Descriptor Type of 2.

Comments on Test Results

a. There were no issues uncovered during the testing process.

Test # and Label	Part(s)	Result(s)
1.4.2: Key Information Field Formatting	**a**	**PASS**
	b	**PASS**
	c	**PASS**

Comments on Test Procedure

Purpose: To verify that the DUT properly formats the Key Information field present in EAPoL-key frames.

The Key Information Field is 2 octets in length and specifies characteristics of the key. The Key Information Field is comprised of the following fields, Key Descriptor Version, Key Type, Reserved, Install, Key MIC, Secure, Error, Request, Encrypted Key Data, SMK Message, and another Reserved. The values that should be contained within each field of the Key Information Field are specified within [1].

The DUT should:
a. set the Key Descriptor Version to 2.
b. set the following bits in the following frames:

Frame	Result
Pairwise Key Message 1	Key Type and Key ACK subfields should be set to 1.
Pairwise Key Message 3	Install, Key Type, Key ACK, the Key MIC, Key Secure and the Encrypted Key Data subfields should all be set to 1.

c. All other bits in the Key Info field should be set to 0.

Comments on Test Results

a-c. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.4.3: Key Length Field Formatting	**a**	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT properly formats the Key Length field present in EAPoL-key frames.

The Key Length Field is 2 octets in length, represented as an unsigned binary number. The value defines the length, in octets, of the PTK to configure into IEEE Std 802.11.

a. The DUT should transmit EAPoL-Key Message 1 and 3 with a Key Length Field of 16.

Comments on Test Results

a. There were no issues uncovered during the testing process.

Test # and Label	Part(s)	Result(s)
1.4.4: Key Replay Counter Formatting	**a**	**FAIL**
	b	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT properly formats the Key Replay Counter field present in EAPoL-key frames.

The Key Replay Counter Field is 8 octets, represented as an unsigned binary number, and is initialized to 0 when the PMK is established. The Supplicant shall use the key replay counter in the received EAPOL-Key frame when responding to an EAPOL-Key frame. It carries a sequence number that the protocol uses to detect replayed EAPOL-Key frames. The Supplicant and Authenticator shall track the key replay counter per security association. The Key Replay Counter shall be initialized to 0 on (re)association. The Authenticator shall increment the key replay counter on each successive EAPOL-Key frame. When replying to a message from the Authenticator, the Supplicant shall use the Key Replay Counter field value from the last valid EAPOL-Key frames received from the Authenticator.

The Authenticator should use the key replay counter to identify invalid messages to silently discard. The Supplicant should also use the Key Replay Counter and ignore EAPOL-Key frames with a Key Replay Counter field value smaller than or equal to any received in a valid message. The local Key Replay Counter field should not be updated until the after EAPOL-Key MIC is checked and is valid. In other words, the Supplicant never updates the Key Replay Counter field for Message 1 in the 4-Way Handshake, as it includes no MIC. This implies the Supplicant must allow for retransmission of Message 1 when checking for the key replay counter of Message 3.

The DUT should:
a. initialize the Key Replay Counter to 0 when the PMK is established.
b. increment the Key Replay Counter on each successive EAPoL-Key frame.

Comments on Test Results

a. The DUT was observed to initialize the Key Replay Counter value to 1 upon successful association. The DUT should initialize the Key Replay Counter to 0 when the PMK is established. See IEEE 802.11-2007 Edition subclause 8.5.2 for more information regarding this test case. Please refer to Table 14 for more information regarding this test case.
b. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.4.5: Key Nonce Field Formatting	**a**	**PASS**
	b	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT properly formats the Key Nonce field present in EAPoL-key frames.

The Key Nonce Field is 32 octets. It conveys the ANonce from the Authenticator and the SNonce from the Supplicant. [1] states that the ANonce and SNonce shall be random or pseudo-random values that shall not repeat for any security association. Choosing the nonces randomly helps prevent precomputation attacks. With unpredictable nonces, a man-in- the-middle attack that uses the Supplicant to precompute messages to attack the Authenticator cannot progress beyond Message 2, and a similar attack against the Supplicant cannot progress beyond Message 3.

The DUT should:
a. use a random or pseudo-random value for the Key Nonce within EAPoL-Key Message 1.
b. use the same value contained within the Key Nonce field of EAPoL-Key Message 1 for the Key Nonce within EAPoL-Key Message 3.

Comments on Test Results

a-b. There were no issues uncovered during the testing process.

Test # and Label	Part(s)	Result(s)
1.4.6: Key IV Field Formatting	**a**	**PASS**
Comments on Test Procedure		

Purpose: To verify that the DUT properly formats the Key IV field present in EAPoL-key frames.

The Key IV Field is 16 octets. It contains the IV used with the KEK. It shall contain 0 when an IV is not required. It should be initialized by taking the current value of the global key counter and then incrementing the counter. Note that only the lower 16 octets of the counter value will be used.

a. The DUT should transmit EAPoL-Key Message 1 and 3 with an EAPoL-Key IV value of 0.

Comments on Test Results

a. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.4.7: Key RSC Field Formatting	**a**	**PASS**
	b	**PASS**

Comments on Test Procedure

Purpose: To verify that the DUT properly formats the Key RSC field present in EAPoL-key frames.

The Key RSC Field is 8 octets in length. It contains the RSC for the GTK being installed in IEEE Std 802.11. It is used in Message 3 of the 4-Way Handshake and Message 1 of the Group Key Handshake, where it is used to synchronize the IEEE 802.11 replay state. It may also be used in the Michael MIC Failure Report frame, to report the TSC field value of the frame experiencing a MIC failure. It shall contain 0 in other messages. The Key RSC field gives the current message number for the GTK, to allow a STA to identify replayed MPDUs. If the Key RSC field value is less than 8 octets in length, the remaining octets shall be set to 0. The least significant octet of the TSC or PN should be in the first octet of the Key RSC field.

The DUT should:
a. transmit EAPoL-Key Message 1 with a RSC value or zero.
b. transmit EAPoL-Key Message 3 with a RSC value equal to the current broadcast/multicast TK and RSC6 and RSC7 should be set to 0.

Comments on Test Results

a-b. There were no issues uncovered during the testing process.

Test # and Label	Part(s)	Result(s)
1.4.8: Reserved Octets Field Formatting	**a**	**PASS**

Comments on Test Procedure

Purpose: To verify that the DUT properly formats reserved octets present in EAPoL-key frames.

[1] states that reserved bits should be set to 0 upon transmission and ignored upon reception.

a. The DUT should transmit EAPoL-Key Message 1 and 3 with all reserved field values set to zero.

Comments on Test Results

a. There were no issues uncovered during the testing process.

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.4.9: Key MIC Field Formatting	**a**	**PASS**
	b	**PASS**
Comments on Test Procedure		
Purpose: To verify that the DUT properly formats the MIC field present in EAPoL-key frames. The Key MIC Field is 16 octets in length when the Key Descriptor Version subfield is 1 or 2. The EAPOL-Key MIC is a MIC of the EAPOL-Key frames, from and including the EAPOL protocol version field to and including the Key Data field, calculated with the Key MIC field set to 0. If the Encrypted Key Data subfield (of the Key Information field) is set, the Key Data field is encrypted prior to computing the MIC. The DUT should: a. set the Key MIC to 0 on EAPoL-Key Message 1. b. set the Key MIC to the correct calculated value in EAPoL-Key Message 3.		
Comments on Test Results		
a-b. There were no issues uncovered during the testing process.		

SAMPLE REPORT

Test # and Label	Part(s)	Result(s)
1.4.10: Key Data & Length Field Formatting	**a**	**Not Applicable**
	b	**PASS**

Comments on Test Procedure

Purpose: To verify that the DUT properly formats the Key Data Length and Key Data fields present in EAPoL-key frames.

The Key Data Length Field is 2 octets in length, taken to represent an unsigned binary number. This represents the length of the Key Data field in octets. If the Encrypted Key Data subfield (of the Key Information field) is set, the length is the length of the Key Data field after encryption, including any padding.

The Key Data Field is a variable-length field that is used to include any additional data required for the key exchange that is not included in the fields of the EAPOL-Key frame. The additional data may be zero or more information element(s) (such as the RSN information element) and zero or more key data cryptographic encapsulation(s) (KDEs) (such as GTK(s) or PMKID(s)). Information elements sent in the Key Data field include the Element ID and Length subfields. KDEs shall be encapsulated.

If the Encrypted Key Data subfield (of the Key Information field) is set, the entire Key Data field shall be encrypted. If the Key Data field uses the NIST AES key wrap, then the Key Data field shall be padded before encrypting if the key data length is less than 16 octets or if it is not a multiple of 8. The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received EAPOL-Key message, the receiver shall ignore this trailing padding. Key Data fields that are encrypted, but do not contain the GroupKey or SMK KDE, shall be accepted.

a. Pairwise Message 1 should be formatted as follows:
   - The Key Data field should contain an unencrypted PMKID KDE.
   - The KDE type field should be set to 0xdd.
   - The PMKID KDE Length field should be 20.
   - The PMKID KDE OUI should be 00-0f-ac.
   - The PMKID Data type field should be 4.
   - The PMKID should be the encapsulated PMKID for the PMK in use.

b. Pairwise Message 3 should be formatted as follows:
   - The Key Data field should contain an RSN IE identical to the RSN IE in the Beacon and Probe Response frames transmitted by the DUT.
   - If an optional 2nd RSN IE is included, the RSN IE should be identical to the 1st except for a single pairwise cipher and a single AKMP.
   - The entire Key Data field should be encrypted.
   - Any pad bytes appended to an Encrypted Key Data field should be included in the Key Data Length field.
   - The Key Data field should be padded with 0xdd and zero or more 0x00 if the Key Data is less than 16 octets or is not a multiple of 8 octets.

   If an optional GTK KDE is included:
   - The KDE type field should be set to 0xdd.
   - The GTK KDE Length field should be 22.
   - The GTK KDE OUI should be 00-0f-ac.
   - The GTK KDE Data type field should be 1.
   - The GTK KDE Key ID field should not be 0.
   - The GTK KDE TX field should be set to 0 in an ESS.
   - The GTK KDE reserved bits should be set to 0 on transmission.
   - The GTK KDE encapsulated key should be 16 octets.

SAMPLE REPORT

Comments on Test Results
a. The DUT did not contain any Key Data Field information in the EAPoL-Key Message 1 frame, therefore KDE type and PMKID parameters could not be verified. b. There were no issues uncovered during the testing process.

SAMPLE REPORT

Trace Evaluation:

Table 3

Test#1.3.2: Key Information Field Processing part b
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.2.apc

No.	Info.	Protocol	Source	Destination
589	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
590	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
591	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
592	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
593	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
594	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
595-603	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
604	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
605	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

```
Frame 593
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 44
    Frame check sequence: 0xbc3962f0 [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 117
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x210a
        .... .... .... .010 = Key Descriptor Version (2)
        .... .... .... 1... = Key Type: Pairwise key
        .... .... ..00 .... = Key Index: 0
        .... .... .0.. .... = Install flag: Not set
        .... .... 0... .... = Key Ack flag: Not set
        .... ...1 .... .... = Key MIC flag: Set
        .... ..0. .... .... = Secure flag: Not set
        .... .0.. .... .... = Error flag: Not set
        .... 0... .... .... = Request flag: Not set
        ...0 .... .... .... = Encrypted Key Data flag: Not set

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa c0 02 aa aa 03 00 00 00 88 8e
0020  02 03 00 75 02 21 0a 00 00 00 00 00 00 00 00 00
0030  01 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0040  0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050  1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 12 b6 5e af 6f a6 c9 74 03 4a 96 14 a1 0a 29
0080  2e 00 16 30 14 01 00 00 0f ac 04 01 00 00 0f ac
0090  04 01 00 00 0f ac 02 28 00 bc 39 62 f0
```

SAMPLE REPORT

Table 4

Test#1.3.2: Key Information Field Processing part c
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.2.apc

No.	Info.	Protocol	Source	Destination
4853	Key #3	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
4854	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
4855	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
4856	Key #4	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
4857	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
4858-4902	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
4902	Echo (ping) request	ICMP	192.168.1.101	192.168.1.20
4903	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
4904	Clear-to-send	IEEE 802.11		aa:bb:cc:dd:ee
4905	Echo (ping) reply	ICMP	192.168.1.20	192.168.1.101

```
Frame 4856
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 399
    Frame check sequence: 0x88cdf96c [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 95
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x070a
        .... .... .... .010 = Key Descriptor Version (2)
        .... .... .... 1... = Key Type: Pairwise key
        .... .... ..00 .... = Key Index: 0
        .... .... .0.. .... = Install flag: Not set
        .... .... 0... .... = Key Ack flag: Not set
        .... ...1 .... .... = Key MIC flag: Set
        .... ..1. .... .... = Secure flag: Set
        .... .1.. .... .... = Error flag: Set
        ...0 0... .... .... = Request flag: Not set
        ...0 .... .... .... = Encrypted Key Data flag: Not set

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa f0 18 aa aa 03 00 00 00 88 8e
0020  02 03 00 5f 02 07 0a 00 00 00 00 00 00 00 00 00
0030  02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 95 71 17 e6 dd 2c 47 2f 1f 42 7c e2 0c a0 3e
0080  94 00 00 88 cd f9 6c
```

SAMPLE REPORT

Table 5

Test#1.3.3: Key Length Field Processing part a
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.3.apc

No.	Info.	Protocol	Source	Destination
399	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
400	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
401	Key #3	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
402	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

```
Frame 399
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
        Flags: 0x1
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 28
    Frame check sequence: 0xe6fe3dde [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 117
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x010a
    Key Length: 32
    Replay Counter: 1
    Nonce: 000102030405060708090A0B0C0D0E0F1011121314151617...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 2C90BC2033FE839E7C4A48E444835BDF
    WPA Key Length: 22
    WPA Key: 30140100000FAC040100000FAC040100000FAC022800

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa c0 01 aa aa 03 00 00 00 88 8e
0020  02 03 00 75 02 01 0a 00 20 00 00 00 00 00 00 00
0030  01 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0040  0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050  1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 2c 90 bc 20 33 fe 83 9e 7c 4a 48 e4 44 83 5b
0080  df 00 16 30 14 01 00 00 0f ac 04 01 00 00 0f ac
0090  04 01 00 00 0f ac 02 28 00 e6 fe 3d de
```

Table 6

Test#1.3.3: Key Length Field Processing part b
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.3.apc

No.	Info.	Protocol	Source	Destination
1696	Key #3	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
1697	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
1798	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
1699	Key #4	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
1700	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
1701-1745	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
1746	Echo (ping) request	ICMP	192.168.1.101	192.168.1.20
1747	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
1748	Clear-to-send	IEEE 802.11		aa:bb:cc:dd:ee
1749	Echo (ping) reply	ICMP	192.168.1.20	192.168.1.101
1750	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

```
Frame 1699
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 125
    Frame check sequence: 0x578aa793 [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 95
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x030a
    Key Length: 16
    Replay Counter: 2
    Nonce: 0000000000000000000000000000000000000000000000000...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 0504FD046EC0440AF419BB3DB463E77A
    WPA Key Length: 0

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa d0 07 aa aa 03 00 00 00 88 8e
0020  02 03 00 5f 02 03 0a 00 10 00 00 00 00 00 00 00
0030  02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 05 04 fd 04 6e c0 44 0a f4 19 bb 3d b4 63 e7
0080  7a 00 00 57 8a a7 93
```

SAMPLE REPORT

Table 7

Test#1.3.5: Key Nonce Field Processing
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.5.apc

No.	Info.	Protocol	Source	Destination
394	Key #3	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
395	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
396	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
397	Key #4	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
398	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
399	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
400-444	…			
445	Echo (ping) request	ICMP	192.168.1.101	192.168.1.20
446	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
447	Clear-to-send	IEEE 802.11		aa:bb:cc:dd:ee
448	Echo (ping) reply	ICMP	192.168.1.20	192.168.1.101
449	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

- Frames 400-444 have been removed for more clarity.

```
Frame 397
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee)
    Fragment number: 0
    Sequence number: 29
    Frame check sequence: 0xdfc20afd [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 95
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x030a
    Key Length: 0
    Replay Counter: 2
    Nonce: 000102030405060708090A0B0C0D0E0F1011121314151617...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 68F860A59B8F7E8244EA2E80A50C7308
    WPA Key Length: 0

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa d0 01 aa aa 03 00 00 00 88 8e
0020  02 03 00 5f 02 03 0a 00 00 00 00 00 00 00 00 00
0030  02 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0040  0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050  1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 68 f8 60 a5 9b 8f 7e 82 44 ea 2e 80 a5 0c 73
0080  08 00 00 df c2 0a fd
```

Table 8

Test#1.3.6: Key IV Field Processing
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.6.apc

No.	Info.	Protocol	Source	Destination
184	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
185	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
186	Key #3	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
187	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

```
Frame 184
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 12
    Frame check sequence: 0xff45e6ff [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 117
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x010a
    Key Length: 0
    Replay Counter: 1
    Nonce: 000102030405060708090A0B0C0D0E0F1011121314151617...
    Key IV: 000102030405060708090A0B0C0D0E0F
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 02B99147D45840023EBDDDC2969CC073
    WPA Key Length: 22
    WPA Key: 30140100000FAC040100000FAC040100000FAC022800

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa c0 00 aa aa 03 00 00 00 88 8e
0020  02 03 00 75 02 01 0a 00 00 00 00 00 00 00 00 00
0030  01 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0040  0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050  1f 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0060  0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 02 b9 91 47 d4 58 40 02 3e bd dd c2 96 9c c0
0080  73 00 16 30 14 01 00 00 0f ac 04 01 00 00 0f ac
0090  04 01 00 00 0f ac 02 28 00 ff 45 e6 ff
```

Table 9

Test#1.3.7: Key RSC Field Processing
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.7.apc

No.	Info.	Protocol	Source	Destination
190	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
191	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
192	Key #3	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
193	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

```
Frame 190
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 12
    Frame check sequence: 0x486fb720 [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 117
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x010a
    Key Length: 0
    Replay Counter: 1
    Nonce: 000102030405060708090A0B0C0D0E0F1011121314151617...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0001020304050607
    WPA Key ID: 0000000000000000
    WPA Key MIC: BC79B03AA09367499816A477745AC954
    WPA Key Length: 22
    WPA Key: 30140100000FAC040100000FAC040100000FAC022800

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa c0 00 aa aa 03 00 00 00 88 8e
0020  02 03 00 75 02 01 0a 00 00 00 00 00 00 00 00 00
0030  01 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0040  0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050  1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 01 02 03 04 05 06 07 00 00 00 00 00 00 00
0070  00 bc 79 b0 3a a0 93 67 49 98 16 a4 77 74 5a c9
0080  54 00 16 30 14 01 00 00 0f ac 04 01 00 00 0f ac
0090  04 01 00 00 0f ac 02 28 00 48 6f b7 20
```

Table 10

Test#1.3.11: Key Data Field Processing (Pairwise Message2) part a
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.11.apc

No.	Info.	Protocol	Source	Destination
227	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
228	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
229-331	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
232	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
233	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
234	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
235	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
236-244	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
245	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
246	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

```
Frame 232
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 12
    Frame check sequence: 0x31c022fe [correct]
802.1X Authentication
    Key Information: 0x010a
    Key Length: 0
    Replay Counter: 1
    Nonce: 000102030405060708090A0B0C0D0E0F1011121314151617...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 43E22316FC156129E55150E651D2B616
    WPA Key Length: 48

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa c0 00 aa aa 03 00 00 00 88 8e
0020  02 03 00 81 02 01 0a 00 00 00 00 00 00 00 00 00
0030  01 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0040  0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050  1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 43 e2 23 16 fc 15 61 29 e5 51 50 e6 51 d2 b6
0080  16 00 30 30 14 01 00 00 0f ac 04 01 00 00 0f ac
0090  04 01 00 00 0f ac 02 28 00 fe 0a 00 01 02 03 04
00a0  05 06 07 08 09 31 c0 22 fe
```

SAMPLE REPORT

Table 11

Test#1.3.11: Key Data Field Processing (Pairwise Message2) part b
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.11.apc c

No.	Info.	Protocol	Source	Destination
451	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
452	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
453-454	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
455	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
456	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
457-466	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
467	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
468	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

```
Frame 455
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 31
    Frame check sequence: 0x99a8e979 [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 124
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x010a
    Key Length: 0
    Replay Counter: 1
    Nonce: 000102030405060708090A0B0C0D0E0F1011121314151617...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 5571E4FD57F16183595C8A917A5933B4
    WPA Key Length: 48
[Malformed Packet: EAPOL]
    [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
        [Message: Malformed Packet (Exception occurred)]
        [Severity level: Error]
        [Group: Malformed]

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa f0 01 aa aa 03 00 00 00 88 8e
0020  02 03 00 7c 02 01 0a 00 00 00 00 00 00 00 00 00
0030  01 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0040  0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050  1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 55 71 e4 fd 57 f1 61 83 59 5c 8a 91 7a 59 33
0080  b4 00 30 30 14 01 00 00 0f ac 04 01 00 00 0f ac
0090  04 01 00 00 0f ac 02 28 00 dd 00 00 00 00 00 00
00a0  99 a8 e9 79
```

SAMPLE REPORT

Table 12

Test#1.3.11: Key Data Field Processing (Pairwise Message2) part c
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.11.apc

No.	Info.	Protocol	Source	Destination
658	Association Request, SSID=MAC""	IEEE 802.11	Xerox_00:00:01	aa:bb:cc:dd:ee
659-662	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
663	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
664	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
665-667	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
668	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
669	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
670-678	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
679	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
680	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
681-690	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast

```
Frame 658
IEEE 802.11 Association Request
    Type/Subtype: Association Request (0x00)
    Frame Control: 0x0000 (Normal)
    Duration: 258
    Destination address: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    BSS Id: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 48
    Frame check sequence: 0xb1d31fd3 [correct]
        Listen Interval: 0x0000
    Tagged parameters (43 bytes)
        SSID parameter set: "MAC"
            Tag Number: 0 (SSID parameter set)
            Tag length: 3
            Tag interpretation: MAC
        Supported Rates: 1.0 2.0 5.5 11.0 6.0 12.0 24.0
            Tag Number: 1 (Supported Rates)
            Tag length: 7
            Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 6.0 12.0
24.0  [Mbit/sec]
        RSN Information
            Tag Number: 48 (RSN Information)
            Tag length: 20
            Tag interpretation: RSN IE, version 1
            Tag interpretation: Multicast cipher suite: AES (CCM)
            Tag interpretation: # of unicast cipher suites: 1
            Tag interpretation: Unicast cipher suite 1: AES (CCM)
            Tag interpretation: # of auth key management suites: 1
            Tag interpretation: auth key management suite 1: PSK
            RSN Capabilities: 0x0028
                .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter
does not support pre-authentication
                .... .... .... ..0. = RSN No Pairwise capabilities:
Transmitter can support WEP default key 0 simultaneously with Pairwise key
                .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4
replay counters per PTKSA/GTKSA/STAKeySA (0x0002)
                .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4
replay counters per PTKSA/GTKSA/STAKeySA (0x0002)
```

SAMPLE REPORT

```
        Extended Supported Rates: 9.0 18.0 36.0 48.0 54.0
            Tag Number: 50 (Extended Supported Rates)
            Tag length: 5
            Tag interpretation: Supported rates: 9.0 18.0 36.0 48.0 54.0
[Mbit/sec]

0000  00 00 02 01 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa 00 03 11 00 00 00 00 03 4d 41
0020  43 01 07 02 04 0b 16 0c 18 30 30 14 01 00 00 0f
0030  ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02 28 00
0040  32 05 12 24 48 60 6c b1 d3 1f d3

Frame 668
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 49
    Frame check sequence: 0x68a81c5e [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 117
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x010a
    Key Length: 0
    Replay Counter: 1
    Nonce: 000102030405060708090A0B0C0D0E0F1011121314151617...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 8D8D8E1C58698D01EBD89DA281BB8034
    WPA Key Length: 24

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa 10 03 aa aa 03 00 00 00 88 8e
0020  02 03 00 75 02 01 0a 00 00 00 00 00 00 00 00 00
0030  01 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0040  0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050  1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 8d 8d 8e 1c 58 69 8d 01 eb d8 9d a2 81 bb 80
0080  34 00 18 30 14 01 00 00 0f ac 04 01 00 00 0f ac
0090  04 01 00 00 0f ac 02 00 00 68 a8 1c 5e
```

SAMPLE REPORT

Table 13

Test#1.3.12: Key Data Field Processing (Pairwise Message4) part c
From: Vendor\Model\July09\MAC\TGi\Traces\1.3.12.apc

No.	Info.	Protocol	Source	Destination
615	Key #4	EAPOL	192.168.1.101	aa:bb:cc:dd:ee
616	Acknowledgement	IEEE 802.11		192.168.1.101 (RA)
617-626	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
627	Key #3	EAPOL	aa:bb:cc:dd:ee	192.168.1.101
628	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

```
Frame 615
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Normal)
    Duration: 44
    BSS Id: aa:bb:cc:dd:ee
    Source address: Xerox_00:00:01 (00:00:01:00:00:01)
    Destination address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 45
    Frame check sequence: 0xe68ef177 [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 119
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x030a
    Key Length: 0
    Replay Counter: 2
    Nonce: 0000000000000000000000000000000000000000000000000...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 2E0653E0047D5F149B5E2C88AB2DBF53
    WPA Key Length: 24
    WPA Key: DD0AFFFFFF05000102030405DD0A0F0F0F05000102030405
        Vendor Specific: ff:ff:ff
            Tag Number: 221 (Vendor Specific)
            Tag length: 10
            Vendor: ff:ff:ff
            Tag interpretation: Not interpreted
        Vendor Specific: 0f:0f:0f

0000  08 01 2c 00 00 1b 63 2d 00 fa 00 00 01 00 00 01
0010  00 1b 63 2d 00 fa d0 02 aa aa 03 00 00 00 88 8e
0020  02 03 00 77 02 03 0a 00 00 00 00 00 00 00 00 00
0030  02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 2e 06 53 e0 04 7d 5f 14 9b 5e 2c 88 ab 2d bf
0080  53 00 18 dd 0a ff ff ff 05 00 01 02 03 04 05 dd

0090  0a 0f 0f 0f 05 00 01 02 03 04 05 e6 8e f1 77
```

SAMPLE REPORT

Table 14

Test#1.4.4: Key Replay Counter Formatting
From: Vendor\Model\July09\MAC\TGi\Traces\1.4.4.apc

No.	Info.	Protocol	Source	Destination
65	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
66	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
67-68	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
69	Key #2	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
70	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
71	Key #3	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
72	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee
73-74	Beacon frames, BI=100, SSID=MAC""	IEEE 802.11	aa:bb:cc:dd:ee	Broadcast
75	Acknowledgement	IEEE 802.11		Xerox_00:00:01 (RA)
76	Key #4	EAPOL	Xerox_00:00:01	aa:bb:cc:dd:ee
77-169	…			
170	Key #1	EAPOL	aa:bb:cc:dd:ee	Xerox_00:00:01
171	Acknowledgement	IEEE 802.11		aa:bb:cc:dd:ee

- The Frames 77-169 have been removed for clarity.

```
Frame 65
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0208 (Normal)
    Duration: 0
    Destination address: Xerox_00:00:01 (00:00:01:00:00:01)
    BSS Id: aa:bb:cc:dd:ee
    Source address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 2
    Frame check sequence: 0xf4140f57 [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 95
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    Nonce: A32AC5CCFDF16CAB6FEC52C9E58693A7DB1B793068CBAF2B...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Length: 0

0000  08 02 00 00 00 00 01 00 00 01 00 1b 63 2d 00 fa
0010  00 1b 63 2d 00 fa 20 00 aa aa 03 00 00 00 88 8e
0020  02 03 00 5f 02 00 8a 00 10 00 00 00 00 00 00 00
0030  01 a3 2a c5 cc fd f1 6c ab 6f ec 52 c9 e5 86 93
0040  a7 db 1b 79 30 68 cb af 2b 72 95 d3 cc 7c 05 a5
0050  a1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080  00 00 00 f4 14 0f 57
```

```
Frame 170
IEEE 802.11 Data
    Type/Subtype: Data (0x20)
    Frame Control: 0x0208 (Normal)
    Duration: 0
    Destination address: Xerox_00:00:01 (00:00:01:00:00:01)
    BSS Id: aa:bb:cc:dd:ee
    Source address: aa:bb:cc:dd:ee
    Fragment number: 0
    Sequence number: 2
    Frame check sequence: 0xd103873b [correct]
802.1X Authentication
    Version: 2
    Type: Key (3)
    Length: 95
    Descriptor Type: EAPOL RSN key (2)
    Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    Nonce: CAB7A60343381D2FF9125BB89378B47338116421CA859247...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Length: 0

0000  08 02 00 00 00 00 01 00 00 01 00 1b 63 2d 00 fa
0010  00 1b 63 2d 00 fa 20 00 aa aa 03 00 00 00 88 8e
0020  02 03 00 5f 02 00 8a 00 10 00 00 00 00 00 00 00
0030  01 ca b7 a6 03 43 38 1d 2f f9 12 5b b8 93 78 b4
0040  73 38 11 64 21 ca 85 92 47 7f fa 37 7e 3b 5b dd
0050  99 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080  00 00 00 d1 03 87 3b
```

SAMPLE REPORT