



# **White paper**

## **Testing for Wi-Fi Protected Access (WPA) in WLAN Access Points**

## Abstract

The vulnerabilities spotted in the Wired Equivalent Privacy (WEP) algorithm used in Wireless LANs have resulted in a lot of industry effort in making Wireless LAN systems more secure. The Wireless Ethernet Compatibility Alliance (WECA) has introduced the WiFi Protected Access (WPA) as a stop-gap solution, based on the draft standard IEEE 802.11i for Enhanced Security in Wireless LANs. This whitepaper provides a description of WPA and Testing of WLAN Access Points for WPA.

## Background

When IEEE introduced the 802.11 Wireless LAN standard in 1999, it provided for the Open System and Shared Key modes of Authentication, while allowing for expansion to other authentication modes.

Though IEEE explicitly recognized that WLAN medium is insecure and is likely to be compromised by casual eavesdropping, it did not mandate any particular authentication scheme and left it to implementors to determine a suitable scheme.

The Open System of Authentication is essentially a null authentication algorithm. The Shared Key authentication mode is based on WEP (Wired Equivalent Privacy) algorithm, developed by RSA Inc. Though the intent of the IEEE in defining WEP was only to bring the functionality of the wireless LAN up to the level implicit in wired LAN design, it has nevertheless resulted in a lot of attention from the Academia and the Industry, who pointed out a number of vulnerabilities with the WEP Algorithm.

The primary weakness of the WEP Algorithm is the use of a 24 bit Initialization Vector (IV) – which is too small and wraps-around, allowing an attacker to decipher the data without the knowledge of the key. Another key weakness is that WEP allows an attacker to discover the default key being used by the access point and the client stations, enabling the attacker to decrypt all messages being sent over the encrypted channel. Over time, free packages have been made available on the internet that allow even casual attackers to discover the WEP key.

The vulnerabilities spotted in WEP has resulted in a lot of industry effort in making Wireless LAN systems more secure. Many vendors announced their own security schemes – based on extending the WEP using a longer Initialization vector and per-session keys. The IEEE 802.11i group is defining a Robust Security Network (RSN) as part of its Specification for Enhanced Security. The Wireless Ethernet Compatibility Alliance (WECA)

has in the meantime introduced the WiFi Protected Access (WPA) as a stop-gap solution, based on the draft 802.11 standard. Though Wi-Fi Protected Access is optional for obtaining Wi-Fi Certification currently, it will soon be a mandatory part of the Wi-Fi Certification process.

### Abbreviations and Acronyms

AES	Advanced Encryption Standard
ANonce	Authenticator Nonce
AP	Access Point
BSS	Basic Service Set
IBSS	Independent Basic Service Set
EAP	Extensible Authentication Protocol (RFC 2284)
EAPOL	EAP over LAN (IEEE 802.1X)
EAP-TLS	EAP with Transport Layer Security (RFC 2716)
ESS	Enhanced Service Set
GMK	Group Master Key
GNonce	Group Nonce
GTK	Group Transient Key
CCMP	Counter mode with CBC-MAC Protocol
MIC	Message Integrity Code
MPDU	Medium access control (MAC) Protocol Data Unit
PEAP	Protected EAP
PSK	Pre-Shared Key
PMK	Pairwise Master Key
PRF	Pseudo-random Function
RADIUS	Remote Authentication Dial-In User Service
RSN IE	Robust Security Network Information Element
RSN	Robust Security Network
SNonce	Supplicant Nonce
STA	Station
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
WRAP	Wireless Robust Authenticated Protocol

## Differences between ESS and IBSS LANs

When the WLAN stations are configured as IBSS (i.e., Ad-hoc Mode), communication may be initiated by either Station, without the need for an Access Point (see Figure 1 scenario 1). Each station must define and implement its own security model, and must trust the other stations to implement and enforce a security model compatible with its own (by negotiating the security algorithms).

In an ESS (i.e., Infrastructure Mode), the station initiates all associations, but the Access Point (AP) enforces a uniform security model (see Figure 1 scenario 2).

In a Robust Security Network (RSN) ESS (see Figure 1 scenario 3), the AP offloads the authentication decision to an authentication server, while in an IBSS each station must make its own authentication decision regarding each peer and hence has to implement its own Authentication Server.

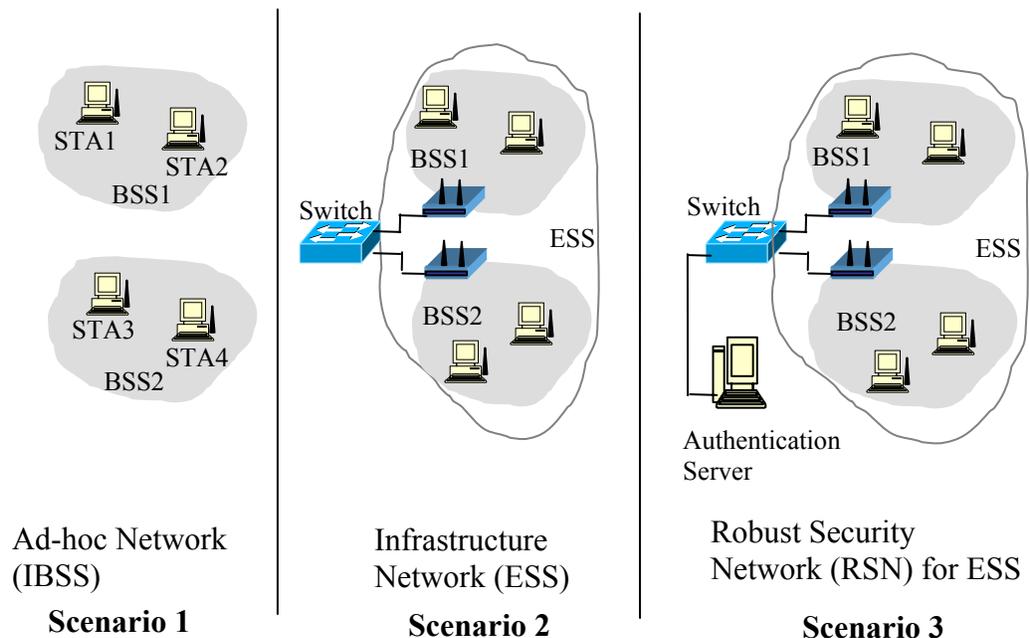


Figure 1 IEEE 802.11 Modes

### Feature support in WPA

Wi-Fi Protected Access (WPA) is a subset of 802.11i draft 3.0 that satisfies some of the requirements of the full 802.11i standard. Some of the significant features of WPA relating to the Access Points are:

- Use of IEEE 802.11 Advertising of supported Cipher suite and Authentication modes along with association and authentication.
- Support for two authenticated key management protocols in infrastructure mode: using 802.1X with pre-shared key and with EAP authentication.
- Support for configuration of the pre-shared key, 802.1X key update interval, Configuration of cipher suites and Configuration of temporal keys.

WPA does not require support for:

- Integrity check on management and control messages.
- Pre-authentication for fast handoff, i.e., Authentication of a Station with the new Access Point, before roaming from the current Access Point, for fast handoff.

### WPA Operation

This section provides a description of WPA operation comprising the following aspects:

- 802.11 Advertisement, Authentication and Association
- 802.1X Authentication
- Key Management
- Data Privacy and Integrity

#### 802.11 Advertisement, Authentication and Association

When the station (STA) becomes active, it searches for APs in radio range using the probe request frames. The probe request frame is sent on every channel the STA supports, in an attempt to find all access points in range that match the SSID and client-requested data rates.

All access points that are in range and match the probe request criteria will respond with a probe response frame containing synchronization information, access point load and security association characteristics, including the authenticated key management, unicast and multicast cipher suites employed (see Figure 2).

The client determines which access point to associate to by weighing the supported data rates, access point load and the security characteristics. Once the client determines the optimal access point to connect to, when WPA is supported, it performs the IEEE 802.11 Open System Authentication and associates to the AP<sup>1</sup>.

At this stage, both the STA and AP, having successfully established a common security policy, filter data traffic, restricting them to IEEE 802.1X EAP authentication frames.

APs/stations should also be capable of being configured to either allow non-WPA stations to associate or to not allow non-WPA stations to associate. When configured to allow association of non-WPA stations, the multicast cipher should be WEP (40 or 104 bit). When configured for WPA, then TKIP with MIC support is the default cryptographic algorithm.

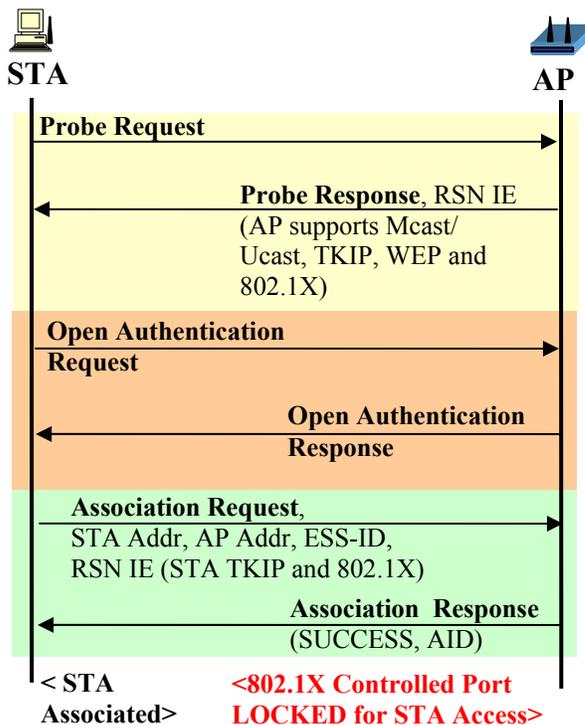


Figure 2 Advertisement, Negotiation of Security characteristics and Association

<sup>1</sup> If Pre-shared key is configured (i.e., AP is working in non-WPA mode), then the AP should use WEP for authentication and for data traffic thereafter. However, Pre-shared key based authentication is insecure and recommended only for home use.

A single IEEE 802.1X Port maps to one association, and each association maps to an IEEE 802.1X Port. After association, the IEEE 802.11 implementation allows any and all data traffic to pass. The IEEE 802.1X Port, however, blocks general data traffic from passing between the STA and the AP until after an IEEE 802.1X authentication procedure is completed. Once IEEE 802.1X authentication is completed, IEEE 802.1X unblocks to allow data traffic.

### **802.1X Authentication**

In this phase, the STA has to successfully authenticate with an Authentication Server (AS). In order for the STA to avoid rogue APs and the AP unauthorized STAs, the STA and AP must mutually authenticate and prove the communication is live and not being replayed. Both the AP and the STA still block general IEEE 802.11 data packets during this phase, allowing only IEEE 802.1X EAP packets to flow.

The IEEE 802.1X authentication step achieves mutual authentication with the STA and derives fresh, never-before-used per-link keys, which are required to protect traffic over the association. The per-link key, known as a Pairwise Transient Key (PTK), is achieved through a protocol called the 4-way handshake.

Once the STA and AP have authenticated and established a fresh pairwise key, the AP can use it to deliver the key required to protect multicast traffic, the Group Transient Key (GTK). This last phase is achieved with a two message exchange, called the Group Key Handshake. Upon its success, both STA and AP open the IEEE 802.1X port and allow communication over a protected channel.

802.11 defines Pre-authentication for fast handoff, so that when the station is attempting to move from one BSS to another, no additional delay is experienced due to authentication with the new AP. WPA does not support Pre-authentication.

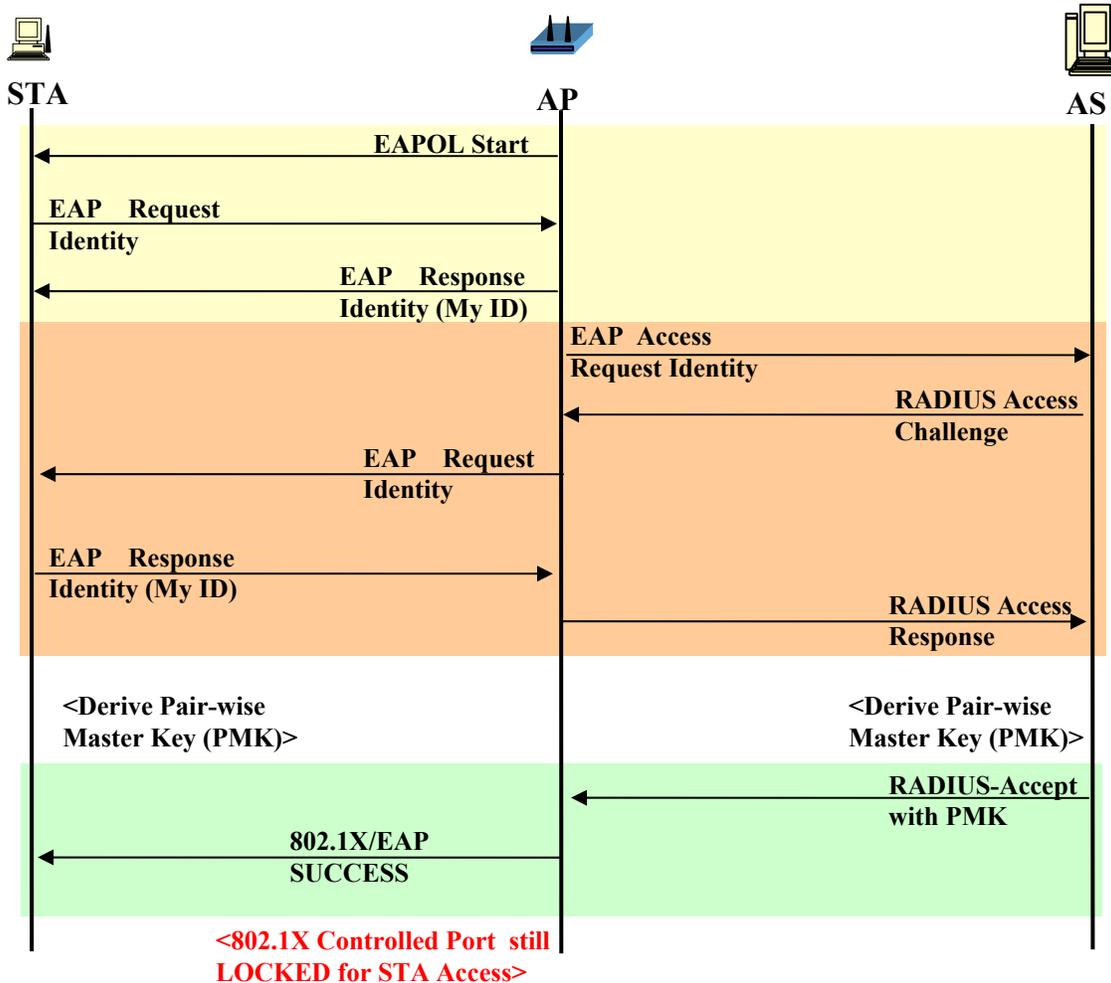


Figure 3 802.1X EAP Authentication

## Key Management

The enhanced privacy, data authentication, and replay protection mechanisms require fresh cryptographic keys. These keys need to be created, distributed, and “aged.” IEEE 802.11 supports two key distribution mechanisms. The first is manual key distribution. The second is automatic key distribution, and is available only in an RSN that uses a IEEE 802.1X to provide key distribution services.

Nonce is a value that is never reused with a key, required to ensure that keys are never reused. A Key Counter (normally 256 bit) is used in the Pseudo-Random Function (PRF) as a nonce to derive Transient Session Keys at the Supplicant and Authenticator – referred to as the SNonce and ANonce respectively. In addition, a Group Nonce is used to derive a Group Transient Key.

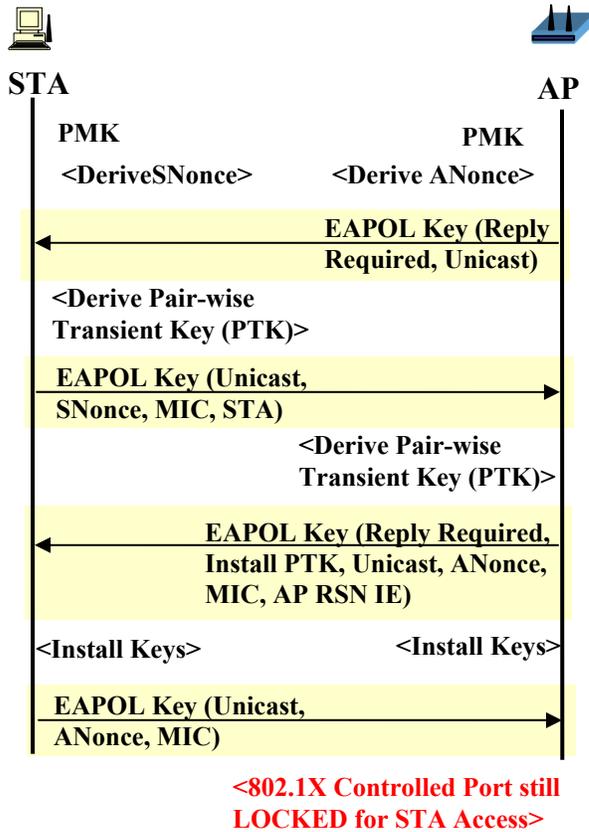


Figure 4 Establishing Pairwise keys

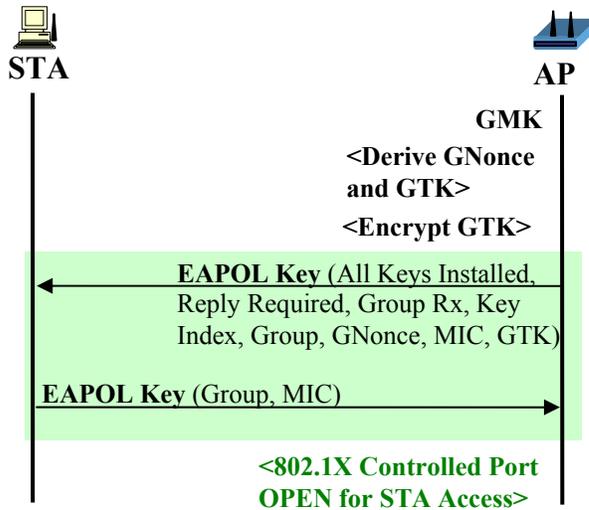


Figure 5 Group key delivery

## Data Privacy and Integrity

IEEE 802.11 provides four cryptographic algorithms to protect data traffic. Two (WEP and TKIP) are based on the RC4 algorithm defined by RSA, and two (WRAP and CCMP) are based on the Advanced Encryption Standard (AES).

WPA supports TKIP with Michael integrity check as the default Cipher, with AES being optional. (Message Integrity Code is a cryptographic digest, designed to make it computationally infeasible for an adversary to alter data). In addition, WPA Access Points should support WEP with and without WEP re-keying.

The data origin authentication mechanism defines a means by which a station that receives a unicast data frame from another station can ensure that the MSDU actually originated from the station whose MAC address is specified in the source address field of the packet. This feature is necessary since an unauthorized station may transmit packets with a source address that belongs to another station. This mechanism is available only to stations using WRAP and TKIP.

The replay detection mechanism defines a means by which a station that receives a unicast data packet from another station can ensure that the packet is not an unauthorized retransmission of a previously sent packet. This mechanism is available only to stations using CCMP, WRAP and TKIP.

## WPA Testing

### AP Management

Functional Testing of the Access Point for WPA should verify for configuration support of all the WPA required parameters such as the Association Methods, Cipher types, Cipher suite parameters, pre-shared keys and temporal keys.

### 802.11 Advertisement, Authentication and Association

If WEP based Association is configured (for compatibility with legacy Stations, without WPA support), the AP should implement the 802.11 Shared Key authentication system, verifying the identity of the Station using the shared, secret, WEP encryption key. Thereafter, all data transfer should use WEP or other supported ciphers. If WEP re-keying is needed, then 802.1X based key management should be supported allowing for refreshing of keys based on set policy for key change (e.g., session based or timer based).

When WPA Association is configured, the AP should advertise WPA availability using the RSN Information Element, with the supported Cipher suites and implement Open Authentication and Association for the Stations. Before Association, the AP should not allow transmission of data frames. After Association, only 802.1X frames should be allowed, other data frames should be dropped. The AP should disable non-WPA clients from associating.

### 802.1X Authentication

In the next phase for WPA, the AP should authenticate the Station, using the services of an Authentication Server. Mutual authentication of the Station and the AP should occur and the station and the AP should derive the Pairwise Master Key (PMK), based on which the Pairwise Transient Key (PTK) should be derived correctly. In this phase, only 802.1X frames should be allowed, other data frames should be dropped.

The AP should use PTK to deliver the Group Transient Key (GTK), using the Group Key Handshake, for multicast traffic. Upon its success, the AP should open the IEEE 802.1X port and allow communication over the protected channel.

### Data Privacy and Integrity

The AP should be verified for correct implementation of TKIP with Michael integrity check for data traffic. In order to be compatible with legacy Stations, the Access Points should also be verified for implementation of encryption with WEP (with and without WEP re-keying) for data traffic.

If AES based ciphers (WRAP, CCMP) are supported, then the AP should be verified for these ciphers also.

### Key Management

The AP should support both manual key distribution and automatic key distribution (using 802.1X). This is required for enhanced privacy, data authentication, and replay protection mechanisms.

**Table 1 Functional Tests for WPA on the AP**

Test	Description
AP Management	Reading and setting of configuration parameters such as Association method (WPA, WEP, WEP Re-keying), WPA Cipher type, Configuration of Cipher suite, etc.
802.11 Authentication Association	Probe Request/Response, Open Authentication, Association, Blocking of port for data frames, Re-association, Roaming, De-authentication
802.1X Authentication	EAPOL authentication with RADIUS-based Authentication Server

Test	Description
Data Integrity /Privacy	WEP, TKIP with Michael MIC If supported - AES (WRAP, CCMP)
Key Management	Manual, Automatic (using 802.1X)
Encrypted/ Un-encrypted Data Handling	Unicast, Multicast, Broadcast data handling in different states and modes

Appendix A gives a list of required/recommended/optional features on the AP for WPA support.

## Conclusion

From the time IEEE introduced the 802.11 Wireless LAN standard in 1999, a lot of industry effort has been spent in making Wireless LAN systems more secure. While the IEEE 802.11i group is defining a Specification for Enhanced Security, the Wireless Ethernet Compatibility Alliance (WECA) has introduced the WiFi Protected Access (WPA) as a stop-gap solution, based on the draft standard IEEE 802.11i. Wireless LAN systems will have to provide support for 802.11i once IEEE standardization is completed.

As more protocols are being added to provide support for more demanding application scenarios, implementors have to ensure conformance to the standards and interoperability with other vendor implementations, with the added challenge of maintaining compatibility with legacy protocols. A comprehensive approach to testing will help address the challenge of releasing consistently well-tested standards-based products in the marketplace. In addition, Automation of the test environment makes testing a manageable and predictable process, apart from savings on resources and time.

## APPENDIX A: WPA Requirements in Access Points

Function	Required/Recommended/Optional
Non-WPA support	Recommended
Non-WPA and WPA mixed mode	Recommended
WPA authentication mode	Required
WPA information element with Privacy bit set in beacon, probe response, association/ re-association request	Required
WPA information element with Privacy bit set in beacon, probe response	Required
Validation of WPA IE in beacon/probe response/ association/ re-association request with WPA IE in 4-way handshake	Required
Open 802.11 MAC authentication for all WPA authentication modes	Required
Group key update	Required
Pairwise Request (with or without error), Group Request (with or without error)	Required
Encryption of 802.1X messages with Pairwise key	Required
802.1X messages not encrypted with Group Keys	Required
No sending of non-802.1X data packets until the correct key is installed.	Required
WPA-Pre Shared Key ASCII passphrase hash	Required
WPA-Pre Shared Key (PSK) - 256 bit key	Recommended

Function	Required/Recommended/Optional
Group key cipher	Required
Pairwise key cipher for AP	Recommended
Group Key Update on a time interval	Recommended
Group key update on a disassociation of a authenticated station	Optional
Use of random number on AP for Master key for Group Key generation	Required
Use of PRF for Pairwise Key generation and Group Key generation	Required
Initialization of Key Counter	Required
Initialization of EAPOL-IV from Key Counter	Required
Queuing of EAPOL-Key messages when in power save	Required
Support for RADIUS in AP	Required
48 bit TKIP (including phase 1 and 2)	Required
Fragmentation of TKIP data packets	Optional
De-fragmentation of TKIP data packets	Required
Use of integrity check and IV for replay protection	Required
Michael MIC	Required
Michael counter measures	Required
Saving of IBSS IV	Required

## APPENDIX B: Relevant Wireless LAN Standards

ANSI/IEEE Std 802.11-1999	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
IEEE Std P802.11i/D3.0	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security (Draft)
Wi-Fi Alliance WPA 2.0	Wi-Fi Protected Access Version 2.0

## About Net-O<sub>2</sub> Technologies

**Net-O<sub>2</sub>** is a dynamic Communications Software company providing innovative tools in the Testing and Test Automation domains. The unique solutions and services from **Net-O<sub>2</sub>** provide customers with tools that drastically reduce “time-required-to-test” and enhance “time-to-market”.

The **Net-O<sub>2</sub> ATTEST** family of automated, “ready-to-use” comprehensive Conformance Test Suites for IP Multicast (PIM, IGMP, DVMRP), IPv6 and Layer-2 Ethernet switch protocols including STP (802.1D), RSTP (802.1w), MSTP (802.1s), VLAN (802.1Q) and Port Based Network Access Control (802.1X). ATTEST’s fully automated solution, provides enhanced capabilities that speed-up the Conformance testing process and help deliver a well-tested product.

For more information please contact [info@net-o2.com](mailto:info@net-o2.com)  
or visit <http://www.net-o2.com/>

