IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

ENCRYPTAWAVE TECHNOLOGIES LLC, Plaintiff, v. **D-LINK CORPORATION,** Defendant.	C.A. No. 4:24-cv-257 **JURY TRIAL DEMANDED** **PATENT CASE**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Encryptawave Technologies LLC files this Original Complaint for Patent Infringement against D-Link Corporation, and would respectfully show the Court as follows:

I. THE PARTIES

1. Plaintiff Encryptawave Technologies LLC ("Encryptawave" or "Plaintiff") is an Illinois limited liability company with its address at 23832 Rockfield Boulevard, Suite 170, Lake Forest, CA 92630.

2. On information and belief, Defendant D-Link Corporation ("Defendant") is a corporation organized and existing under the laws of Taiwan, having its principal place of business at No. 289, Xinhu 3rd Road, Neihu District, Taipei 11494, Taiwan.

II. JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction of such action under 28 U.S.C. §§ 1331 and 1338(a).

4. On information and belief, Defendant is subject to this Court's specific and general personal jurisdiction, pursuant to due process and the Texas Long-Arm Statute, due at least to its

business in this forum, including at least a portion of the infringements alleged herein. Defendant is subject to this Court's general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, Tex. Civ. Prac. & Rem. Code § 17.042, due at least to its substantial business conducted in this District, including: (i) having solicited and transacted business in Texas, including benefits directly related to the instant patent infringement causes of action set forth herein; (ii) having placed its products and services into the stream of commerce throughout the United States and having been actively engaged in transacting business in Texas and in this District, and (iii) having committed the complained of tortious acts in Texas and in this District.

5. In another case in this District, the Court found that it has personal jurisdiction over D-Link based on its stream of commerce involving Wi-Fi products. *Am. Patents LLC v. D-Link Corp.*, Civil Action No. 4:19-cv-764, 2020 U.S. Dist. LEXIS 123158, at *12 (E.D.Tex. July 14, 2020). Specifically, the Court held "the evidence suggests that, even if not the manufacturer of the accused products, D-Link Corp. at the very least has some level of control over the accused products' placement into the stream of commerce that ends in sales in the United States and in Texas that ends in sales of the accused products in the United States and in Texas." *Id.* Further, "the evidence suggests that D-Link Corp. plays a role in furnishing the accused products to DLink International, which then coordinates with D-Link Systems to have those products distributed and sold in the United States, including in Texas. *Id.* at *14. Moreover, "there is evidence that D-Link Corp. seeks out the United States market for sales of the accused products. Product packaging and documentation for some of the accused products is apparently labeled with D-Link Corp. copyrights, as are United States and Texas case studies from D-Link's website—many of which highlight the use of D-Link Corp.'s products in Texas." *Id.* at *15.

6. Without limitation, on information and belief, within this state, Defendant has sold, offered for sale, and/or used the patented inventions thereby committing, and continuing to commit, acts of patent infringement alleged herein. In addition, on information and belief, Defendant has derived revenues from its infringing acts occurring within Texas. Further, on information and belief, Defendant is subject to the Court's general jurisdiction, including from regularly doing or soliciting business, engaging in other persistent courses of conduct, and deriving substantial revenue from goods and services provided to persons or entities in Texas. Further, on information and belief, Defendant is subject to the Court's personal jurisdiction at least due to its sale and offer for sale of products and/or services within Texas. Defendant has committed such purposeful acts and/or transactions in Texas such that it reasonably should know and expect that it could be haled into this Court as a consequence of such activity.

7. Venue is proper in this district under 28 U.S.C. § 1400(b). On information and belief, from and within this District Defendant has committed at least a portion of the infringements at issue in this case. Furthermore, venue is proper as to Defendant because 28 U.S.C. § 1391(c)(3) provides that "a defendant not resident in the United States may be sued in any judicial district, and the joinder of such a defendant shall be disregarded in determining where the action may be brought with respect to other defendants."

8. For these reasons, personal jurisdiction exists, and venue is proper in this Court under 28 U.S.C. § 1400(b).

III. COUNT I
(PATENT INFRINGEMENT OF UNITED STATES PATENT NO. 7,233,664)

9. Plaintiff incorporates the above paragraphs herein by reference.

10. On June 19, 2007, United States Patent No. 7,233,664 ("the '664 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '664 Patent is titled

"Dynamic Security Authentication for Wireless Communication Networks." A true and correct copy of the '664 Patent is attached hereto as Exhibit A and incorporated herein by reference.

11. Encryptawave is the assignee of all right, title, and interest in the '664 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '664 Patent. Accordingly, Encryptawave possesses the exclusive right and standing to prosecute the present action for infringement of the '664 Patent by Defendant.

12. The invention in the '664 Patent relates to the field of wireless communication network security, more particularly to a dynamic authentication method and system for providing secure authentication among wireless communication network nodes. (*Id.* at col. 1:18-22).

13. The objective of cryptography is to allow users to communicate securely through an insecure shared data communications channel while maintaining data integrity, privacy, and user authentication. (*Id.* at col. 1:24-27). Over the past century, cryptographic systems have been developed that require a great deal of time to break, even when using large computational power. (*Id.* at col. 1:27-30). However, once an encryption key is obtained, the encryption mechanism and likely the entire system security is compromised and a new key is required. (*Id.* at col. 1:30-33). The two most common strategies for making an encryption system difficult to penetrate are: (1) a long encryption key, and/or (2) a complex encryption function. (*Id.* at col. 1:34-37). For example, for an encryption key of length *n* bits, for large values of *n* a code breaker would need more than a lifetime to break the cipher. (*Id.* at col. 1:37-39). Simpler encryption functions, such as the logic XOR function, are easy to decipher no matter how long the key length is. (*Id.* at col. 1:39-43). For example, a logic XOR operation is performed on one bit of data and its corresponding bit from the encryption key, one bit at a time: if the bits are the same then the result is 0 and if the bits are

different then the result is 1. (*Id.* at col. 1:43-45). The simple linearity of the XOR function allows an intruder to decipher individual key fragments using a divide-and-conquer approach and then reconstruct the entire key once all the individual fragments are obtained. (*Id.* at col. 1:47-51). A non-linear exponential encryption function, such as Rivest-Sharmi-Adelman (RSA) system, is more difficult to apply a divide-and-conquer approach to break the key. (*Id.* at col. 1:51-54).

14. At the time the patent application was filed, there were two major cryptography system philosophies: 1) symmetric systems (static or semi-dynamic key), and 2) public key systems (static key). (*Id.* at col. 1:55-57). In symmetric systems, a key is exchanged between the users (the sender and receiver) and is used to encrypt and decrypt the data. (*Id.* at col. 1:57-60). There are three main problems with the symmetric system. (*Id.* at col. 1:60-61). First, the exchange of the key between the users introduces a security loophole, which can be alleviated through encrypting the exchanged key using a secure public key cryptography system. (*Id.* at col. 1:61-64). Second, using only one static encryption key makes it easier for an intruder to have sufficient time to break the key, which can be addressed using multiple session keys that are exchanged periodically. (*Id.* at col. 1:64-66). Third, and most important, is the susceptibility to an insider attack on the key where the time window between exchanging keys might be long enough for a super user, who has super user privileges, to break in and steal the key. (*Id.* at col. 2:1-6).

15. In RSA public key cryptography system, a user generates two related keys, reveals one to the public ("public" key) to be used to encrypt any data sent and a second key that is private to the user ("private" key) that is used to decrypt received data by the user. (*Id.* at col. col. 2:7-11). The RSA cryptography system generates large random primes and multiplies them to get the public key and uses a complex encryption function such as mod and exponential operations, which

makes the technique unbreakable in a lifetime for large keys (*e.g.*, higher than 256 bits) and eliminates the problem of insecure exchange of symmetric keys. (*Id.* at col. 2:15-20). However, the huge computational time required by RSA encryption and decryption, in addition to the time to generate the keys, is not appealing to users of the Internet and is therefore mainly used as one-shot solid protection of the symmetric cryptography key exchange. (*Id.* at col. 2:20-25). This one-shot protection, however, allows an internal super user with a helper to generate its own pair of encryption keys and replace the original keys. (*Id.* at col. 2:24-25). The sender then uses the super user's public key so the super user can decrypt the cipher text, store it, re-encrypt it using the original public key to continue the data to the original recipient for decrypting using the original private key without any knowledge of the break that occurred in the middle (a "super-user-in-the-middle" attack). (*Id.* at col. 2:29-40).

16. Even though both symmetric and public key cryptography systems are secure against outside attack, they are still vulnerable to insider attacks. (*Id.* at col. 2:41-48). A common way to protect a static encryption key is to save it under a file with restricted access but this cannot prevent a person with super user privileges from accessing the static key of the host file. (*Id.* at col. 2:50-53). Various attempts have been made to circumvent intrusion by outside users, however, they are still prone to attack by super-user-in-the-middle attacks. (*Id.* at col. 2:53 – col. 3:3). The invention in the '664 patent alleviates these problems by providing continuous encryption key modification. (*Id.* at col. 4:26-29).

17. There was a need for security for wireless communications in networks, including allowing mobile communication devices to move between access ports or base stations while maintaining full, mutually secure authentication. (*Id.* at col. 3:4-12). In wireless local area networks, the Wired Equivalent Privacy (WEP) algorithm is used to protect wireless

communication from eavesdropping. (*Id.* at col. 3:33-36). WEP relies on a secret encryption key that is shared between a supplicant, such as a wireless laptop personal computer, and an access point. (*Id.* at col. 3:36-39). The secret key is used to encrypt data packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. (*Id.* at col. 3:39-41). The standard does not discuss how the shared key is established; however, in practice, most installations use a single key that is shared between all mobile stations and access points. (*Id.* at col. 3:41-44).

18. Ineffective WEP security leads to different types of attacks by outsiders. (*Id.* at col. 3:60-61). For example, a passive eavesdropper can intercept all wireless traffic and through known methodologies and educated guesses can narrow the field of the contents of a message and possibly determine the exact contents of the message. (*Id.* at col. 3:45 – col. 4:6). Another type of attack when using a WEP algorithm is if an attacker knows the exact plaintext for one encrypted message, the attacker can use this knowledge to construct correct encrypted packet. (*Id.* at col. 4:7-17). Therefore, despite the WEP algorithm being part of the standard that describes communications in wireless local area networks, it fails to protect the wireless communications from eavesdropping and unauthorized access to wireless networks, primarily because it relies on a static secret key shared between the supplicant and the wireless network. (*Id.* at col. 4:18-24).

19. There are several benefits to the claimed invention. The key lifetime is too small for an intruder to break and a super-user to copy. (*Id.* at col. 4:29-31). The invention also reduces the computations overhead by breaking the complexity of the encryption function and shifting it over the dynamics of data exchange. (*Id.* at col. 4:32-35). Speed is also improved by using a simple logic encryption function. (*Id.* at col. 4:35-36). Encryption is fully automated and all

parties, the source user, destination user, and central authority, are clock-free synchronized and securely authenticated at all times. (*Id.* at col. 4:44-47).

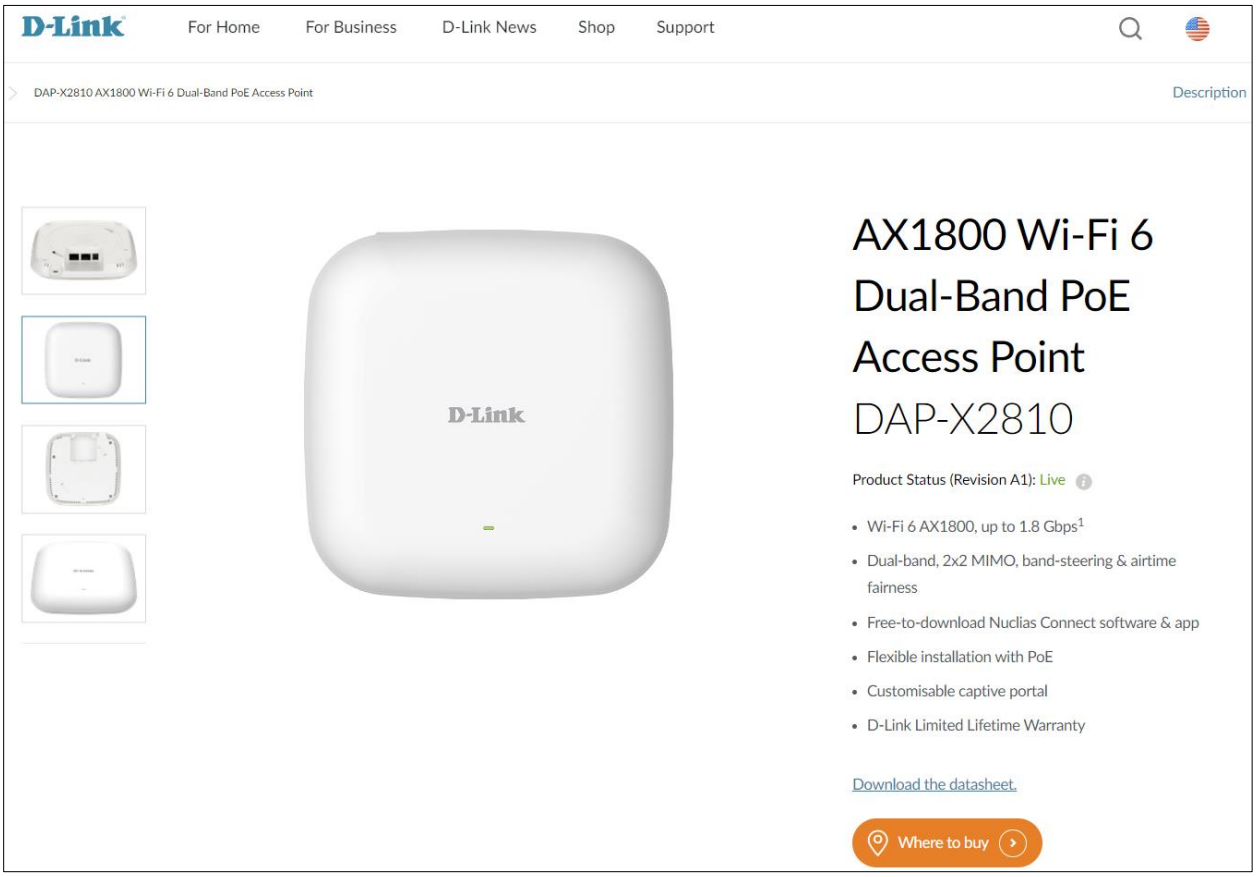
20. The prosecution history of the '664 patent further explains the unconventional features of the claimed invention. The examiner allowed the relevant claims without rejection because the prior art of record did not teach installing a node identifier at a first network node; sending the node identifier information from a first network node to a second network node, and synchronously regenerating an authentication key at two network nodes based upon node identifier information. (Ex. B at 2).

21. **Direct Infringement.** Upon information and belief, Defendant has been directly infringing claim 1 of the '664 patent in Texas, and elsewhere in the United States, by performing actions comprising using or performing the claimed method of providing secure authentication between wireless communication network nodes by using and/or testing the D-Link AX1800 Dual-Band PoE Access Point, Aquila Pro M30, Aquila Pro M30-2, Aquila Pro M60, Aquilla Pro M30/3, AX1800, AX4800, COVR-2202-US, COVR-3902-US, COVR-C1203-US, COVR-L1900, COVR-P2502-US, COVR-X1682, COVR-X1863-CA, DAB-2682, DAP-1260, DAP-1325-US, DAP-1330, DAP-1360, DAP-1530-US, DAP-1610-US, DAP-1620, DAP-1620-EXO, DAP-1650, DAP-1720, DAP-1755-US, DAP-1820-US, DAP-1870, DAP-1950-CA, DAP-1955-US, DAP-2360, DAP-2610, DAP-2662, DAP-2680, DAP-2682, DAP-3320, DAP-3662, DAP-3666, DAP-LX1880-CA, DAP-X1860, DAP-X1870, DAP-X2810, DAP-X2850, DAP-X3060, DBA-1210P, DBA-2520P, DBA-2720P, DBA-2820P, DBA-3620P, DBA-3621P, DBA-X1230P, DBA-X2830P, DIR-1260, DIR-1360-US, DIR-1750-US, DIR-1950-US, DIR-1960-US, DIR-2150-CA, DIR-2640-US, DIR-2660-US, DIR-2680-US, DIR-3040-US, DIR-3060-US, DIR-605L, DIR-819-CA, DIR-821-CA, DIR-822-CA, DIR-822-US, DIR-842, DIR-867-US, DIR-869, DIR-878,

DIR-879, DIR-882-US, DIR-L1900-US, DIR-LX1870, DIR-X1550, DIR-X1560-US, DIR-X1870-US, DIR-X3260, DIR-X4860-US, DIR-X5460-US, DIS-2650AP, DIS-3650AP, DSL-2740B, DSR-1000AC, DWA-121, DWA-131, DWA-137, DWA-171, DWA-172, DWA-181-US, DWA-182, DWA-185, DWA-192, DWA-582, DWA-F18, DWA-X1850, DWA-X3000, DWA-X582, DWL-6610AP/APE, DWL-6620APS, DWL-8620AP/APE, DWL-8630AP, DWL-8720AP, DWM-311-B1, DWP-1010, DWR-2101, DWR-932, DWR-933, DWR-953V2, DWR-960, DWR-961-VZ, DWR-961-VZ-R, DWR-978, E15, E30, Eagle Pro E15, Eagle Pro G403, Eagle Pro G415, Eagle Pro G416, Eagle Pro M15-2/M15-3, Eagle Pro M18, Eagle Pro M32-2/M32-3, Eagle Pro R12, Eagle Pro R15, Eagle Pro R18, Eagle Pro R32, G403, G415, G416, M15, M18, M30, M32, M60, R12, R15, R18, R32, W5BKT1, DIR-835M, DWL-X8630AP, DSL-G2452GR, DAP-2462, DWL-8710AP, DSL-3785, DAP-1120, DAP-1320, DAP-1360, DAP-1513, DAP-1520, DAP-1525, DAP-1533, DAP-1620-EXO, DAP-1860, DAP-2553 REV A, DAP-2555, DAP-2590, DAP-2660, DAP-3520, DAP-3525, DAP-3690, DCH-M225, DIR-330, DIR-505, DIR-505L, DIR-506L, DIR-510L, DIR-605L, DIR-615, DIR-619L-ES, DIR-626L, DIR-636L, DIR-640L, DIR-645, DIR-655, DIR-808L, DIR-810L, DIR-813, DIR-817LW, DIR-830L, DIR-842, DIR-850L, DIR-855L, DIR-859, DIR-860L, DIR-866L, DIR-869, DIR-879, DIR-880L, DIR-885L/R, DIR-890L/R, DIR-895L/R, and GO-RT-N300 (each an "Accused Instrumentality"). (*E.g.*, https://www.dlink.com/us/en/products/dap-x2810-ax1800-wifi-6-dualband-poe-access-point).

The excerpts in this complaint are for the D-Link AX1800 Dual-Band PoE Access Point, however, each of the Accused Instrumentalities supports wireless connection with Wi-Fi networks using WPA2 security, which is based on the IEEE 802.11i standard. The accusation of infringement is therefore the same for each of the Accused Instrumentalities as described below.

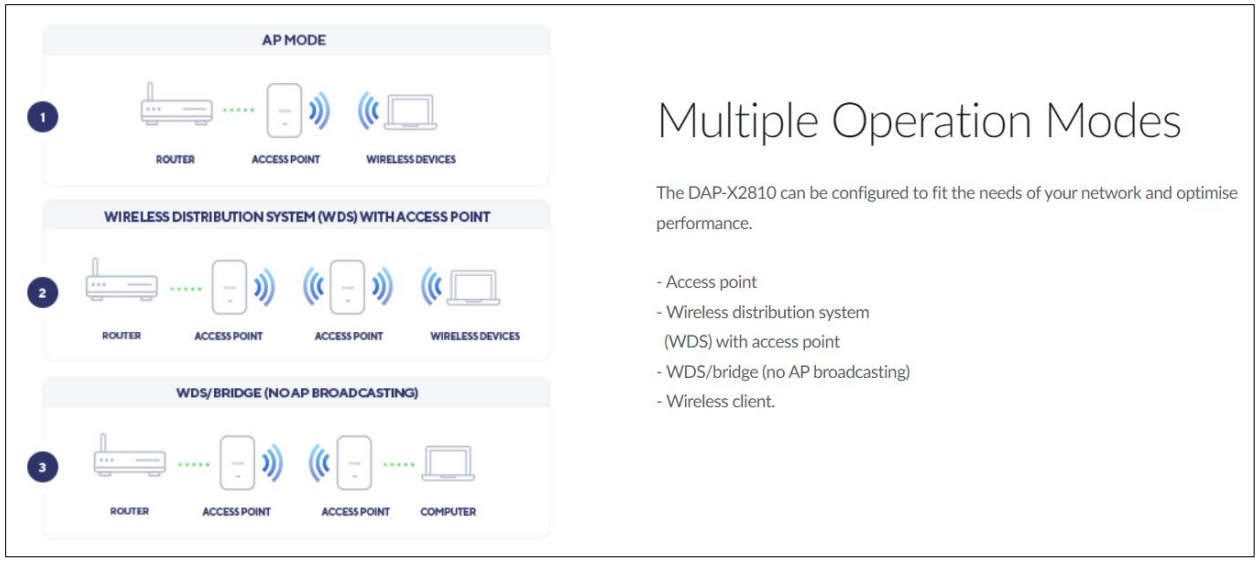
22. For example, a system utilized by the Accused Instrumentality practices a method of providing secure authentication between wireless communication (*e.g.*, Wi-Fi) network nodes (*e.g.*, the Accused Instrumentality and accessory devices such as a Wi-Fi enabled smartphone, etc.). As shown below, the Accused Instrumentality provides wireless connection to accessory devices and allows them to join its Wi-Fi network. The Accused Instrumentality sets a password to secure the Wi-Fi network. The Accused Instrumentality utilizes WPA2 security, which is based on the IEEE 802.11i standard, to set a password.



(*E.g.*, https://www.dlink.com/us/en/products/dap-x2810-ax1800-wifi-6-dualband-poe-access-point).

Functionality	
Standards	IEEE 802.11a/b/g/n/ac/ax, IEEE 802.3u/ab, IEEE 802.3az Energy-Efficient Ethernet (EEE), IEEE 802.3at PoE
Operating Frequency	2.4 - 2.483 GHz, 5.15 - 5.35 GHz, 5.47 - 5.85 GHz
Security Protocol	WPA/WPA2/WPA3™ Personal/Enterprise, WEP 64/128-bit, SSID broadcast disable, MAC address access control, internal RADIUS server

(*E.g.*, https://www.dlink.com/us/en/-/media/business_products/dap/dap-x2810/datasheet/dap_x2810_datasheet_eu_en.pdf).



(*E.g.*, https://www.dlink.com/us/en/products/dap-x2810-ax1800-wifi-6-dualband-poe-access-point).

Wi-Fi Protected Access (WPA / WPA2 / WPA3)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a RADIUS Server on the network for authentication.
WPA-Personal does not require the user to install a RADIUS Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

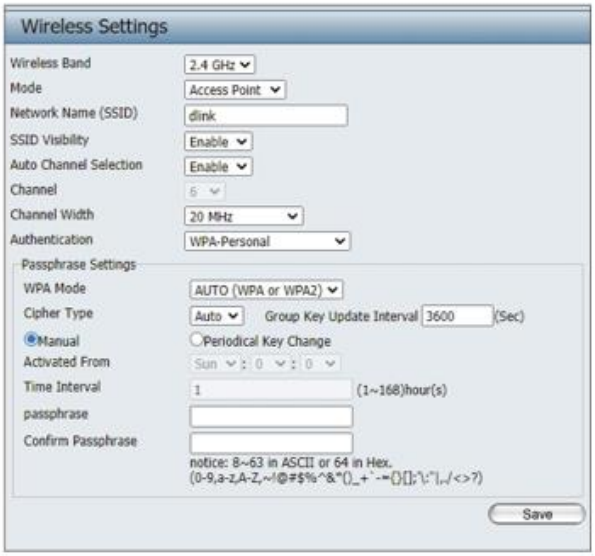
WPA2/WPA3 are upgrades of WPA. WPA2/WPA3 yet again solves some possible security issues found in WPA. WPA2/WPA3 have two variations called WPA2/WPA3-Personal (PSK) and WPA2/WPA3-Enterprise (EAP) which are the same as found with WPA.

WPA Mode: When WPA-Personal is selected for Authentication type, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 or WPA3,WPA2 Only or WPA3 Only.

Cipher Type: When you select WPA-Personal, you must also select AUTO, AES, or TKIP from the drop-down menu.

Group Key Update: Select the interval during which the group key will be valid. The default value of 3600 is recommended.

Pass Phrase: When you select WPA-Personal, enter a Pass Phrase in the corresponding field.



D-Link DAP-X2810 User Manual 18

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).

WPA Mode: When WPA-Enterprise is selected, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2) or WPA2 Only or WPA3 only.

Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.

Group Key Update Interval: Select the interval during which the group key will be valid. 3600 is the recommended value as a lower interval may reduce data transfer rates.

RADIUS Server: Enter the IP address of the RADIUS server to be used in authenticate.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the shared secret to be used between the radius server and the DAP to authenticate.

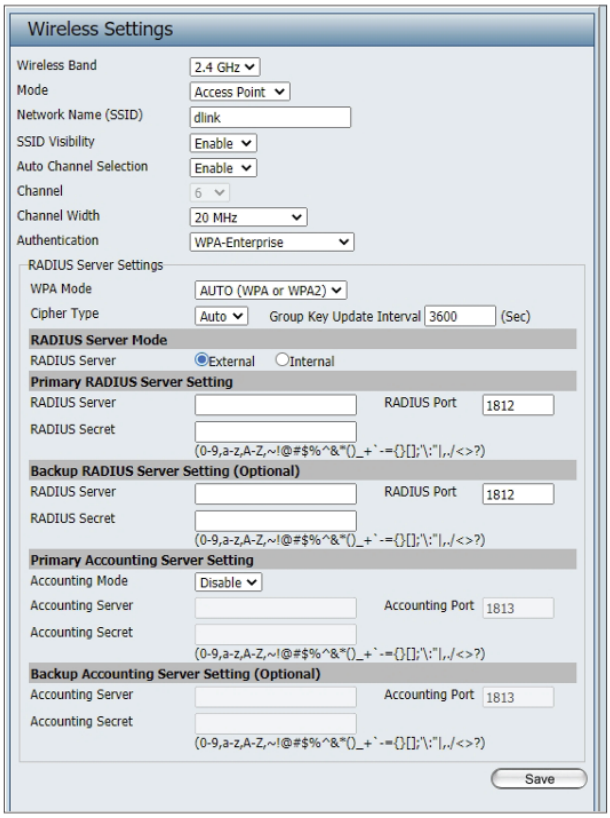
Accounting Mode: Click the drop-down menu to enable or disable the accounting mode.

Accounting Server: Enter the IP address of the accounting server.

Accounting Port: Enter the accounting port.

Accounting Secret: Enter the accounting secret.

Save: Save the updated configuration. Click **Configuration** > **Save and Activate** to make changes permanent.



D-Link DAP-X2810 User Manual 19

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).

Wi-Fi Security: WEP & WPA / WPA2

An overview or tutorial about the IEEE 802.11 standards for Wi-Fi and WLAN applications and the associated WLAN equipment and the use of Wifi hotspots.

WiFi IEEE 802.11 Includes:

Wi-Fi IEEE 802.11 introduction Standards Security How to stay safe on public Wi-Fi Wi-Fi Bands Router location & coverage How to buy the best Wi-Fi router Wi-Fi boosters, range extenders & repeaters Wi-Fi wired & powerline extender

Wi-Fi network security is an issue of importance to all Wi-Fi users. It is defined under the IEEE stadnard 802.11i and security schemes like as WEP, WPA, WPA2 and WPA3 are widely mentioned, with keys or codes being provided for the various Wi-Fi hotspots in use.

Wi-Fi security is of significant importance because very many people use it: at home, in the office and when they are on the move. As the wireless signal can be picked up by non-authorised users, it is imperative to ensure that they cannot access the system.

Even users who legitimately gain access to a system could the try to hack other computers on the same hotspot.

(*E.g.*, https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/security-wep-wpa-wpa2.php).

5.1.1.4 Interaction with other IEEE 802® layers

IEEE Std 802.11 is required to appear to higher layers [logical link control (LLC)] as a wired IEEE 802 LAN. This requires that the IEEE 802.11 network handle STA mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE Std 802.11 to incorporate functionality that is untraditional for MAC sublayers.

In a robust security network association (RSNA), IEEE Std 802.11 provides functions to protect data frames, IEEE Std 802.1X-2004 provides authentication and a Controlled Port, and IEEE Std 802.11 and IEEE Std 802.1X-2004 collaborate to provide key management. All STAs in an RSNA have a corresponding IEEE 802.1X entity that handles these services. This standard defines how an RSNA utilizes IEEE Std 802.1X-2004 to access these services.

(*E.g.*, https://standards.ieee.org/standard/802_11-2007.html).

5.2.3.2 RSNA

An RSNA defines a number of security features in addition to wired equivalent privacy (WEP) and IEEE 802.11 authentication. These features include the following:

- Enhanced authentication mechanisms for STAs
- Key management algorithms
- Cryptographic key establishment
- An enhanced data cryptographic encapsulation mechanism, called Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), and, optionally, Temporal Key Integrity Protocol (TKIP).

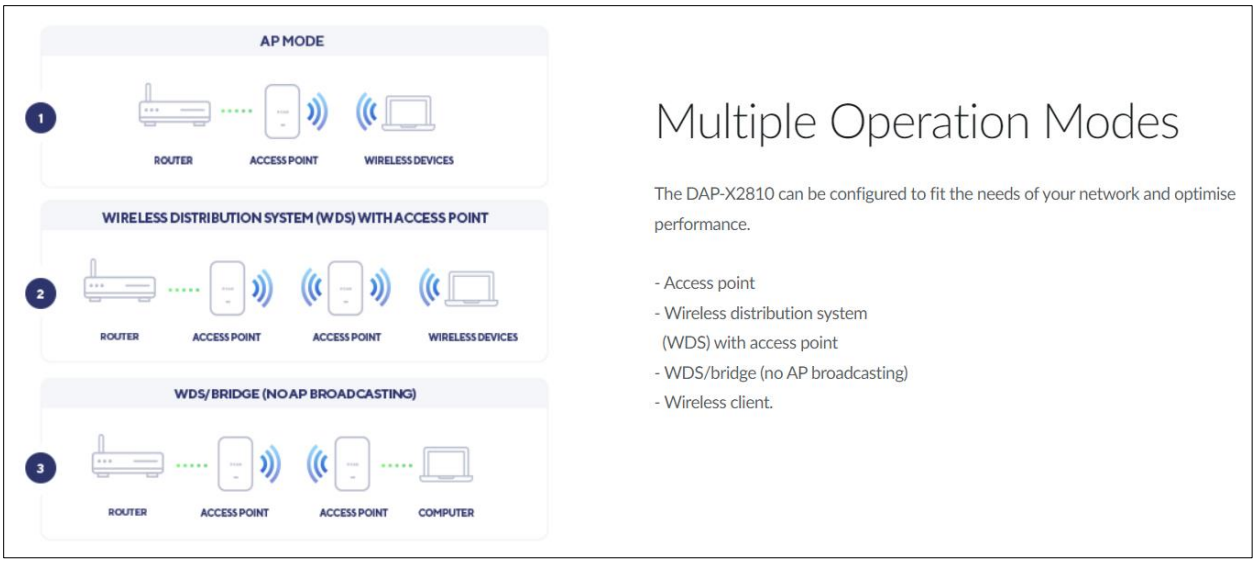
An RSNA relies on several components external to the IEEE 802.11 architecture.

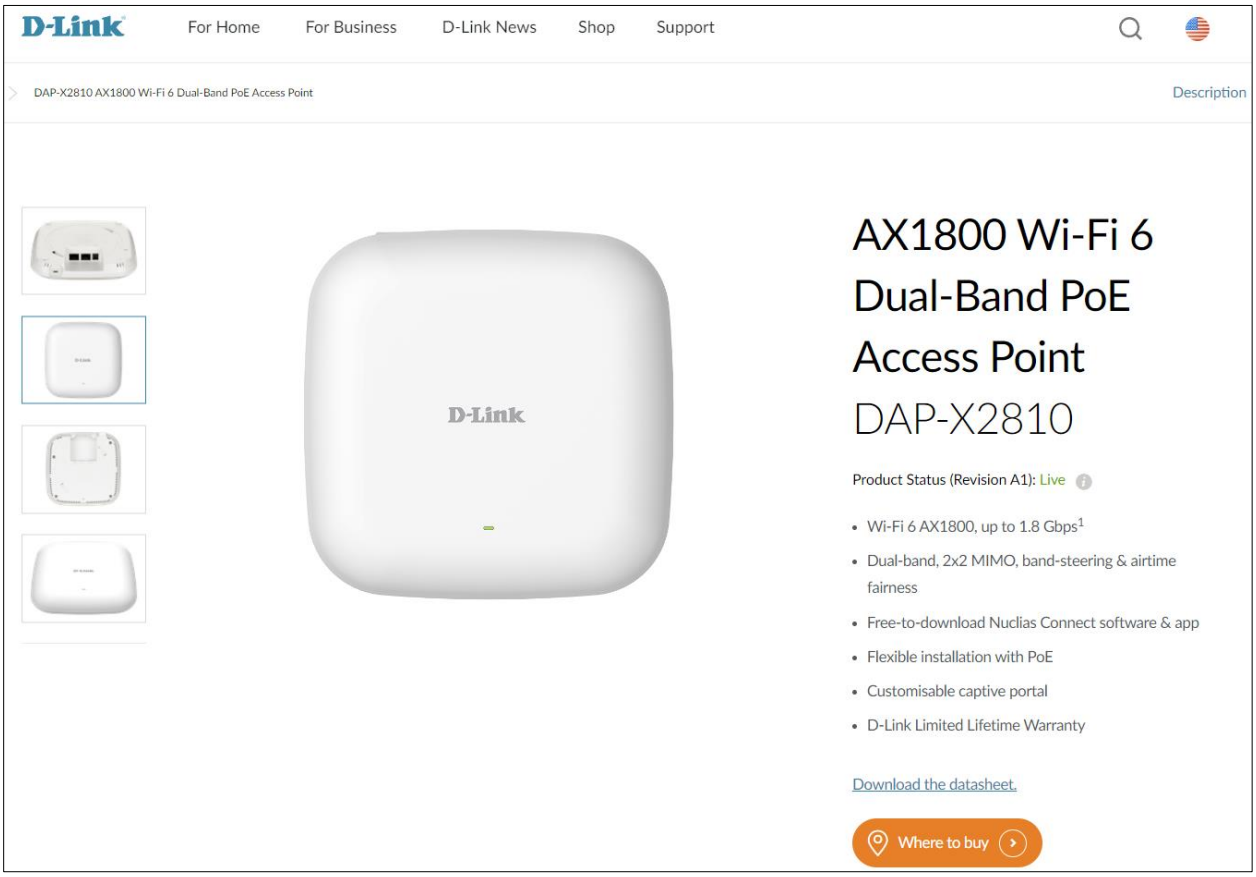
The first component is an IEEE 802.1X port access entity (PAE). PAEs are present on all STAs in an RSNA and control the forwarding of data to and from the medium access control (MAC). An AP always implements the Authenticator PAE and Extensible Authentication Protocol (EAP) Authenticator roles, and a non-AP STA always implements the Supplicant PAE and EAP peer roles. In an IBSS, each STA implements both the Authenticator PAE and Supplicant PAE roles and both EAP Authenticator and EAP peer roles.

A second component is the Authentication Server (AS). The AS may authenticate the elements of the RSNA itself, i.e., the non-AP STAs; and APs may provide material that the RSNA elements can use to authenticate each other. The AS communicates through the IEEE 802.1X Authenticator with the IEEE 802.1X Supplicant on each STA, enabling the STA to be authenticated to the AS and vice versa. An RSNA depends upon the use of an EAP method that supports mutual authentication of the AS and the STA, such as those that meet the requirements in IETF RFC 4017. In certain applications, the AS may be integrated into the same physical device as the AP, or into a STA in an IBSS.

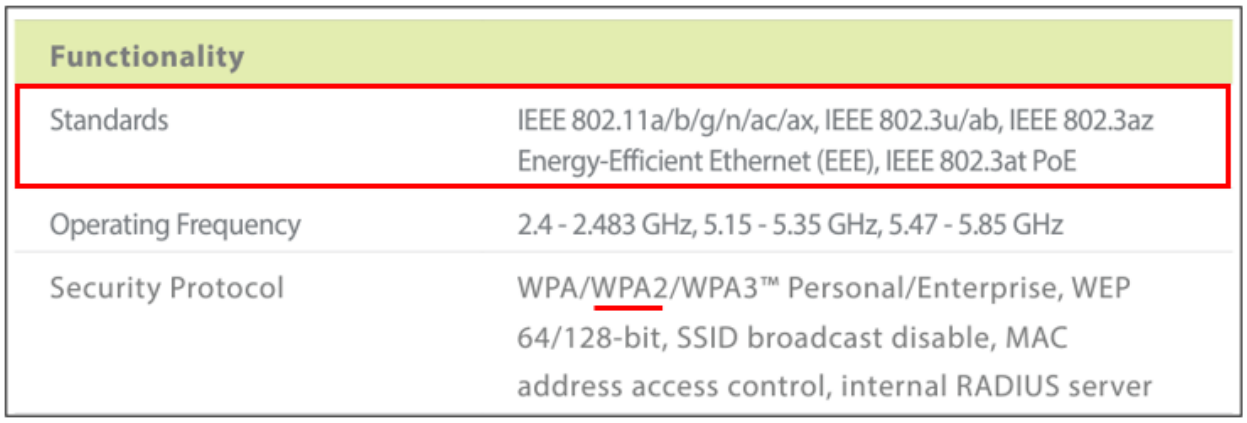
(*E.g.*, https://standards.ieee.org/standard/802_11-2007.html).

23. Upon information and belief, the system utilized by the Accused Instrumentality practices providing a node identifier comprising an address (*e.g.*, MAC address) and an initial authentication key (*e.g.*, Pre-shared key or Pairwise master key). The Accused Instrumentality provides wireless connection to accessory devices (*e.g.*, accessory devices such as a Wi-Fi enabled smartphone, etc.) to join its Wi-Fi network. An accessory device (*e.g.*, accessory devices such as a Wi-Fi enabled smartphone, etc.) is provided with a MAC address (i.e., address of NIC card of the accessory device) and an initial authentication key (*e.g.*, Wi-Fi password which is a pre-shared key or pairwise master key) to join the Wi-Fi network.



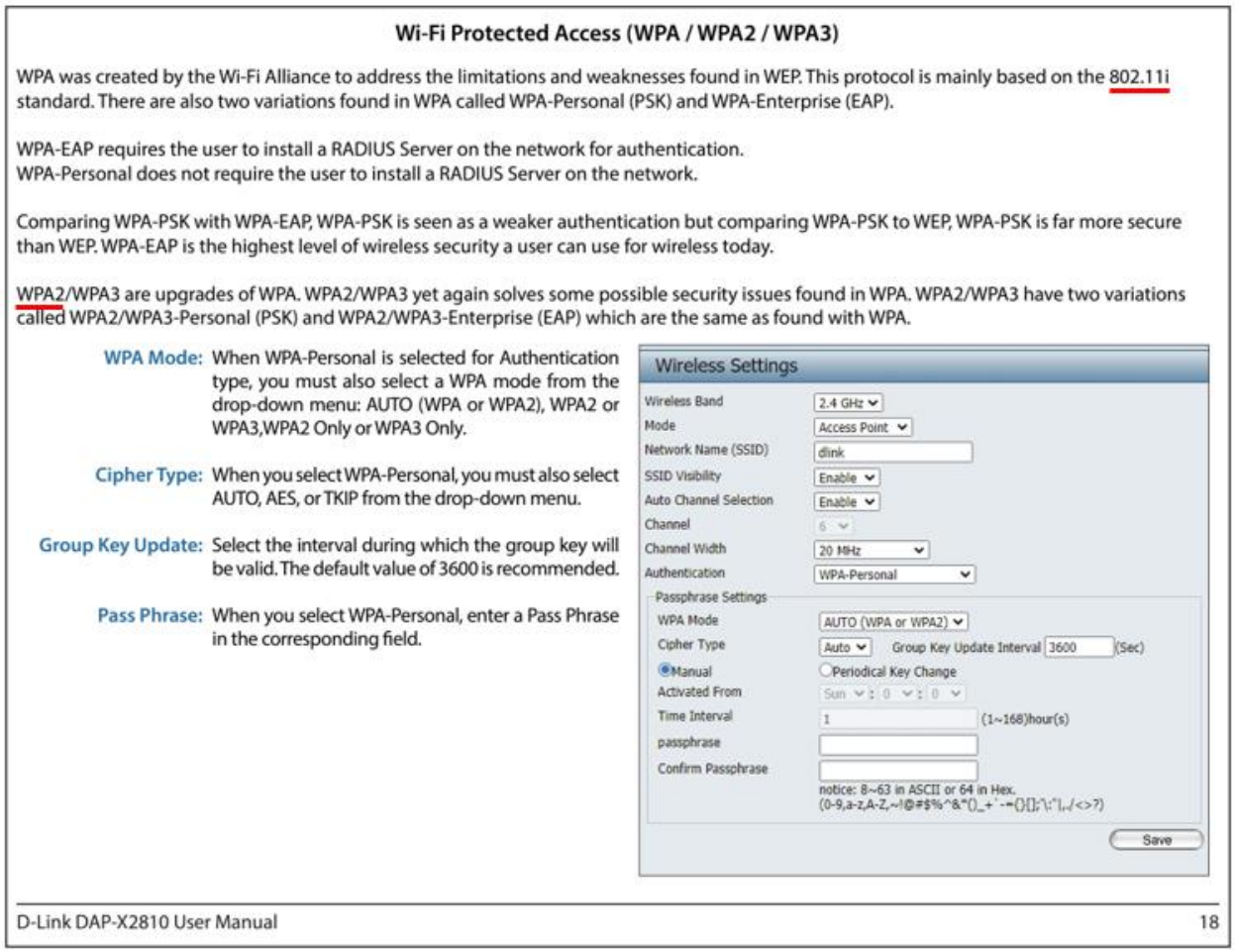


(*E.g.*, https://www.dlink.com/us/en/products/dap-x2810-ax1800-wifi-6-dualband-poe-access-point).



Functionality	
Standards	IEEE 802.11a/b/g/n/ac/ax, IEEE 802.3u/ab, IEEE 802.3az Energy-Efficient Ethernet (EEE), IEEE 802.3at PoE
Operating Frequency	2.4 - 2.483 GHz, 5.15 - 5.35 GHz, 5.47 - 5.85 GHz
Security Protocol	WPA/WPA2/WPA3™ Personal/Enterprise, WEP 64/128-bit, SSID broadcast disable, MAC address access control, internal RADIUS server

(*E.g.*, https://www.dlink.com/us/en/-/media/business_products/dap/dap-x2810/datasheet/dap_x2810_datasheet_eu_en.pdf).



Wi-Fi Protected Access (WPA / WPA2 / WPA3)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a RADIUS Server on the network for authentication.
WPA-Personal does not require the user to install a RADIUS Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

WPA2/WPA3 are upgrades of WPA. WPA2/WPA3 yet again solves some possible security issues found in WPA. WPA2/WPA3 have two variations called WPA2/WPA3-Personal (PSK) and WPA2/WPA3-Enterprise (EAP) which are the same as found with WPA.

WPA Mode: When WPA-Personal is selected for Authentication type, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 or WPA3,WPA2 Only or WPA3 Only.

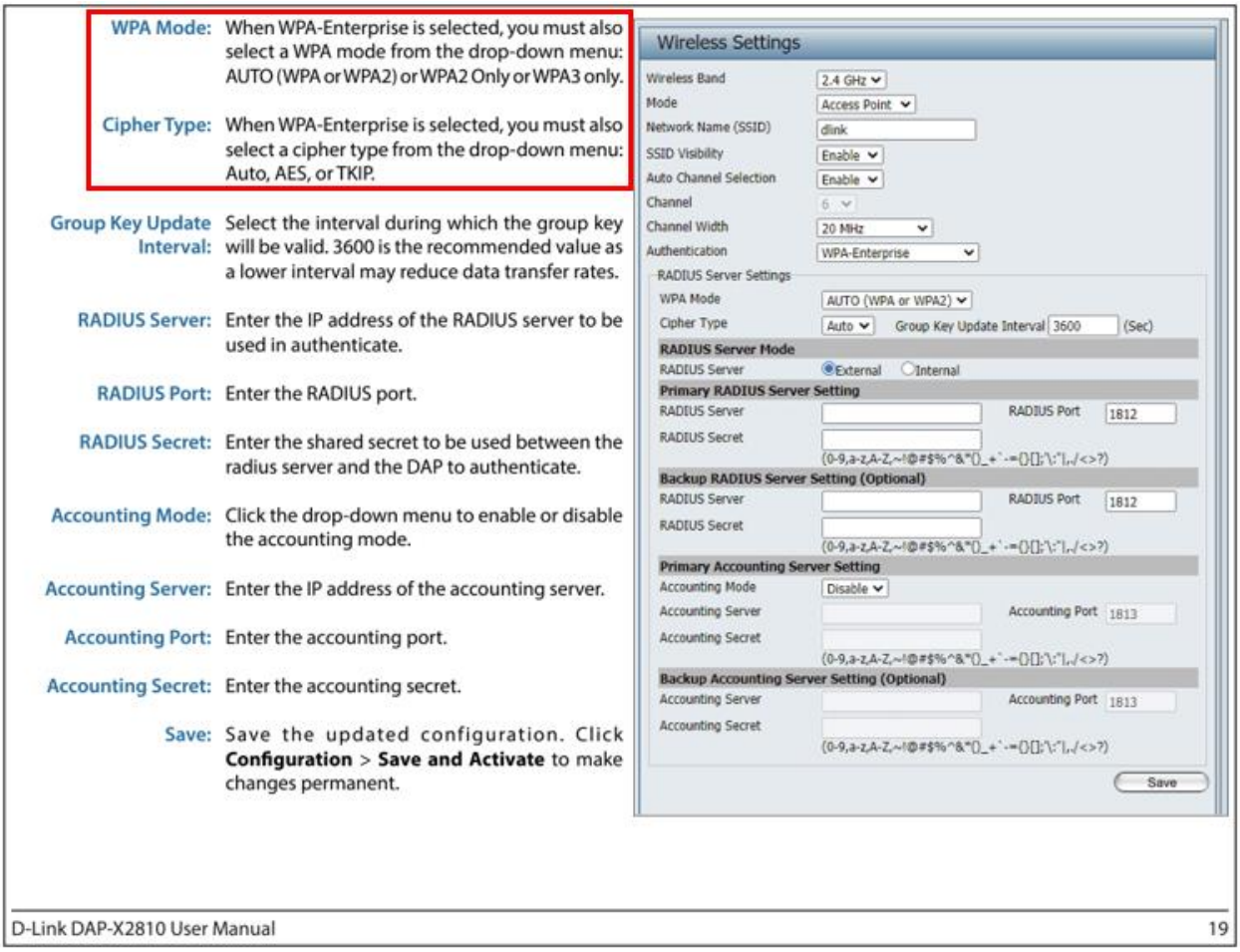
Cipher Type: When you select WPA-Personal, you must also select AUTO, AES, or TKIP from the drop-down menu.

Group Key Update: Select the interval during which the group key will be valid. The default value of 3600 is recommended.

Pass Phrase: When you select WPA-Personal, enter a Pass Phrase in the corresponding field.

D-Link DAP-X2810 User Manual 18

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).



WPA Mode: When WPA-Enterprise is selected, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2) or WPA2 Only or WPA3 only.

Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.

Group Key Update Interval: Select the interval during which the group key will be valid. 3600 is the recommended value as a lower interval may reduce data transfer rates.

RADIUS Server: Enter the IP address of the RADIUS server to be used in authenticate.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the shared secret to be used between the radius server and the DAP to authenticate.

Accounting Mode: Click the drop-down menu to enable or disable the accounting mode.

Accounting Server: Enter the IP address of the accounting server.

Accounting Port: Enter the accounting port.

Accounting Secret: Enter the accounting secret.

Save: Save the updated configuration. Click **Configuration** > **Save and Activate** to make changes permanent.

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).

So not surprisingly, along with an IP address (which is networks software), there's also a hardware address. Typically it is tied to a key connection device in your computer called the network interface card, or NIC. The NIC is essentially a computer circuit card that makes it possible for your computer to connect to a network.

An NIC turns data into an electrical signal that can be transmitted over the network.

Hey Nick. Meet Mac.

Every NIC has a hardware address that's known as a MAC, for Media Access Control. Where IP addresses are associated with TCP/IP (networking software), MAC addresses are linked to the hardware of network adapters.

A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it. Something called the ARP (Address Resolution Protocol) translates an IP address into a MAC address. The ARP is like a passport that takes data from an IP address through an actual piece of computer hardware.

(*E.g.*, https://whatismyipaddress.com/mac-address).

- 802.11 frames have up to four address fields in the MAC header.
- 802.11 frames typically use only three of the MAC address fields (4 in WDS environment).

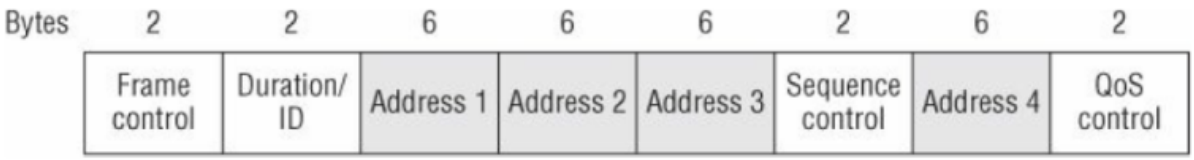


Figure 9.3 802.11 MAC header

(*E.g.*, https://dot11ap.wordpress.com/ieee-802-11-frame-format-vs-ieee-802-3-frame-format/).

Depending on whether the 802.11 traffic is upstream or downstream, the definition of each of the four MAC address fields in the layer 2 header will change.

The five definitions are as follows:

- **Source Address (SA)** The MAC address of the original sending station is known as the SA. The source address can originate from either a wireless station or the wired network.
- **Destination Address (DA)** The MAC address that is the final destination of the layer 2 frame is known as the DA. The final destination may be a wireless station or could be a destination on the wired network such as a server or a router.

(*E.g.*, https://dot11ap.wordpress.com/ieee-802-11-frame-format-vs-ieee-802-3-frame-format/).

WPA-PSK

WPA-PSK uses this kind of key-encryption system to protect Wi-Fi networks. When you set a WPA-PSK password on the router, you are actually setting the key which the WPA standard will use to encrypt data. When users type in this matching key as their "password" their computers will be able to communicate with the router. Otherwise, they can't join the network because their computers will be incapable of understanding anything the router sends them. There is no such thing as a "default" key in key-based encryption methods. If your router is broadcasting with WPA-PSK, it means that someone with administrative access to the router enabled encryption with a key of his own choosing.

(*E.g.*, https://smallbusiness.chron.com/default-wpapsk-wifi-39458.html).

IEEE 802.11 defines two authentication methods: Open System authentication and Shared Key authentication. Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA also supports authentication based on IEEE 802.1X, or preshared keys (PSKs). IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This amendment does not specify an EAP method that is mandatory to implement. See 8.4.4 for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

In an RSNA, IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port.

(*E.g.*, IEEE 802.11i).

5.9.2.2 Operations with PSK

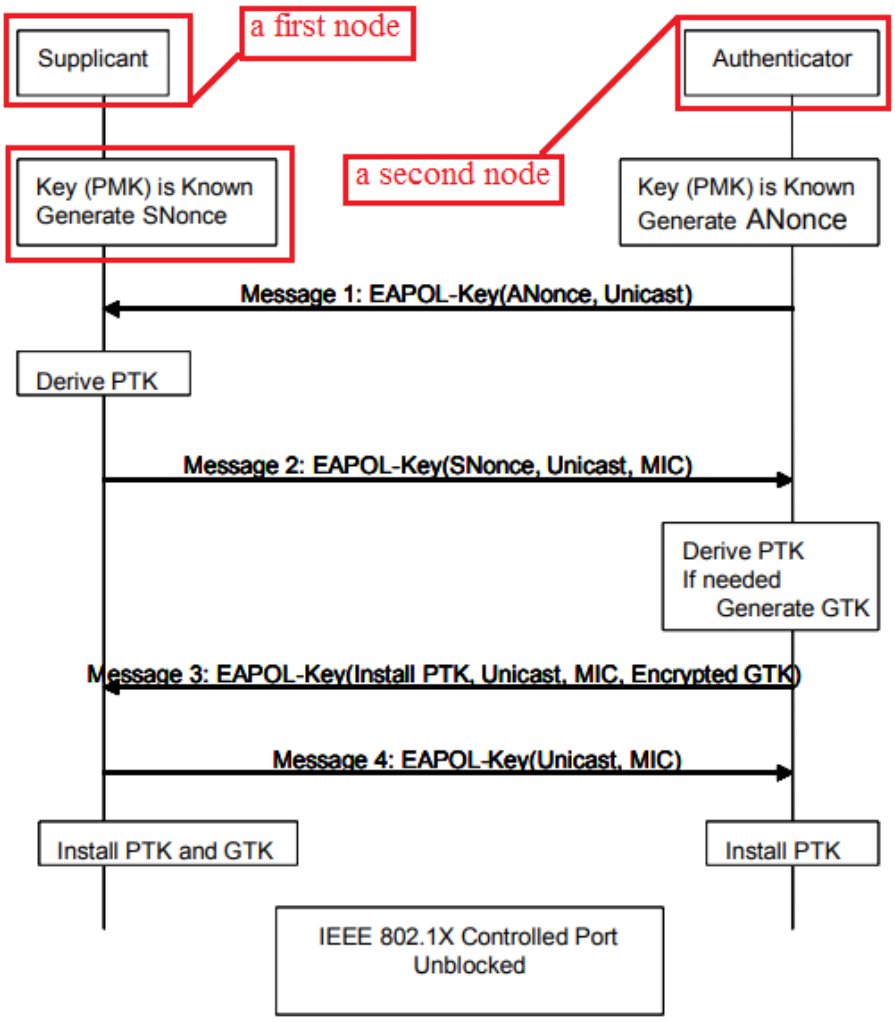
The following AKM operations are carried out when the PMK is a PSK:

— A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing (shown in Figure 11a). A STA associates with an AP and negotiates a security policy. The PMK is the PSK.

— The 4-Way Handshake using EAPOL-Key frames is used just as with IEEE 802.1X authentication, when an AS is present. See Figure 11c.

— The GTK and GTK sequence number are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 11c and Figure 11d.

(*E.g.*, IEEE 802.11i).



(*E.g.*, IEEE 802.11i).

b) If an RSNA is based on a PSK in an ESS, the STA's SME establishes an RSNA as follows:

1) It identifies the AP as RSNA-capable from the AP's Beacon or Probe Response frames.

2) It shall invoke Open System authentication.

3) It negotiates cipher suites during the association process, as described in 8.4.2 and 8.4.3.

4) It establishes temporal keys by executing a key management algorithm, using the protocol defined by 8.5. It uses the PSK as the PMK.

5) It protects the data link by programming the negotiated cipher suites and the established temporal key into the MAC and then invoking protection.

c) If an RSNA is based on a PSK in an IBSS, the STA's SME executes the following sequence of procedures:

1) It identifies the peer as RSNA-capable from the peer's Beacon or Probe Response frames.

NOTE—STAs may respond to a data MPDU from an unrecognized STA by sending a Probe Request frame to find out whether the unrecognized STA is RSNA-capable.

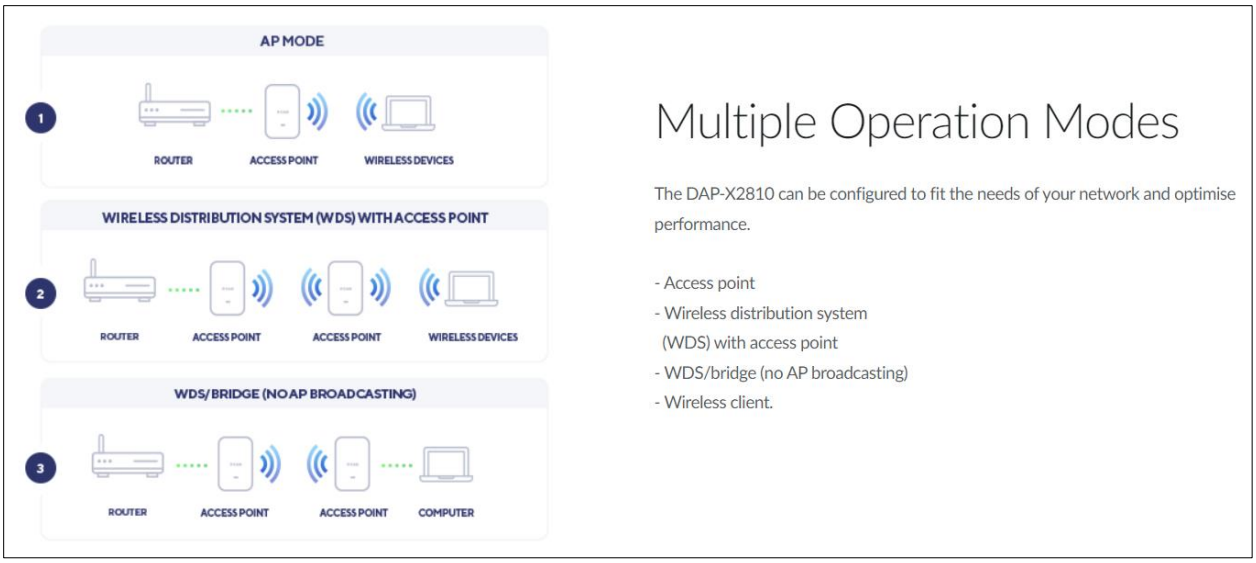
2) It may optionally invoke Open System authentication.

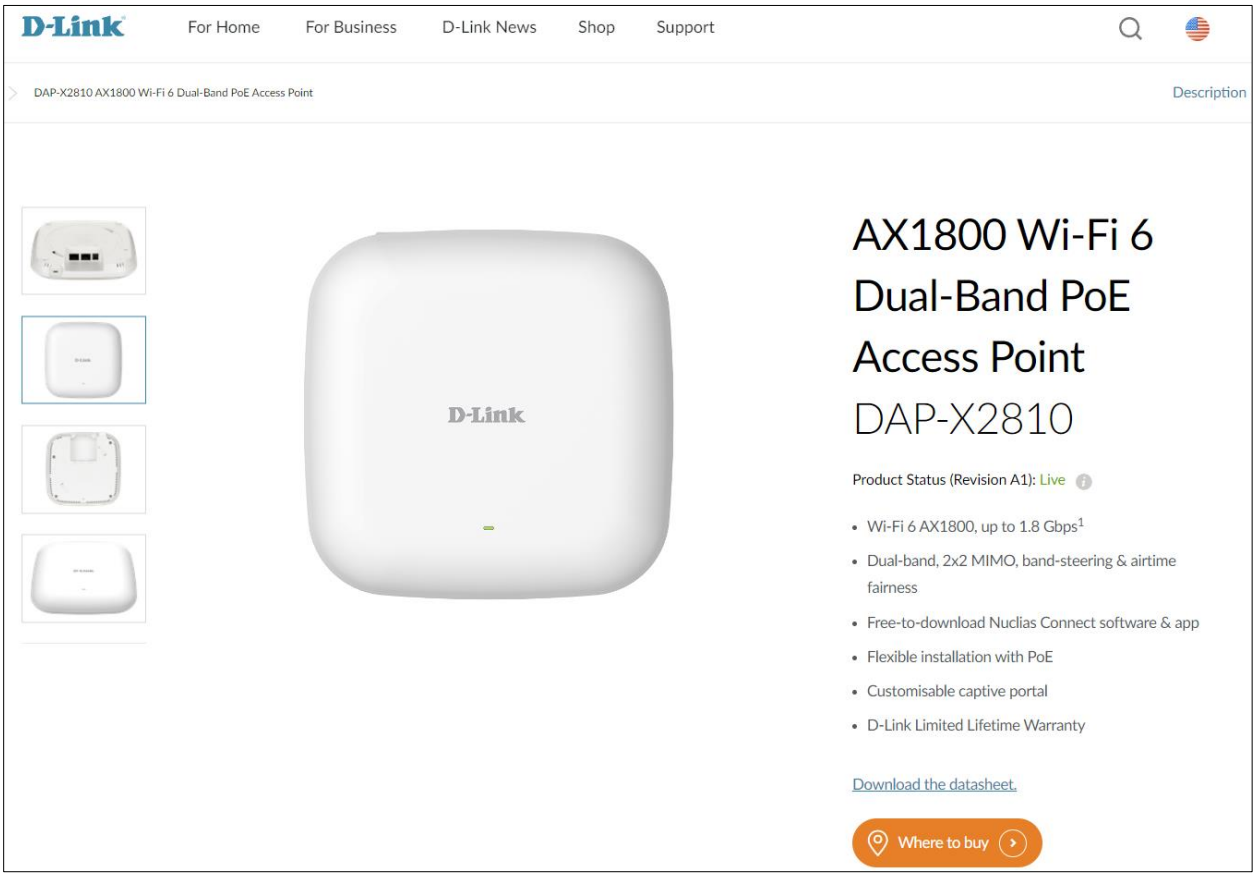
3) Each STA uses the procedures in 8.5, to establish temporal keys and to negotiate cipher suites. It uses a PSK as the PMK. Note that two peer STAs may follow this procedure simultaneously. See 8.4.9.

4) It protects the data link by programming the negotiated cipher suites and the established temporal key and then invoking protection.

(*E.g.*, IEEE 802.11i).

24. Upon information and belief, the system utilized by the Accused Instrumentality practices installing the node identifier (*e.g.*, MAC address and pre-shared key or pairwise master key) at a first network node (*e.g.*, accessory devices such as a Wi-Fi enabled smartphone, etc.). A MAC address of an accessory device is a hardware address of a network interface card of an accessory device (*e.g.*, accessory device such as a Wi-Fi enabled smartphone, etc.). Also, the accessory device needs to utilize a Wi-Fi password which is pre-shared key or pairwise master key (*e.g.*, initial authentication key) of the wireless connection of the Accused Instrumentality to join the Wi-Fi network. Upon information and belief, the accessory device enters or installs the Wi-Fi password as well as the MAC address in the Wi-Fi stack of the accessory device to initiate an association process with the Wi-Fi network of the Accused Instrumentality.

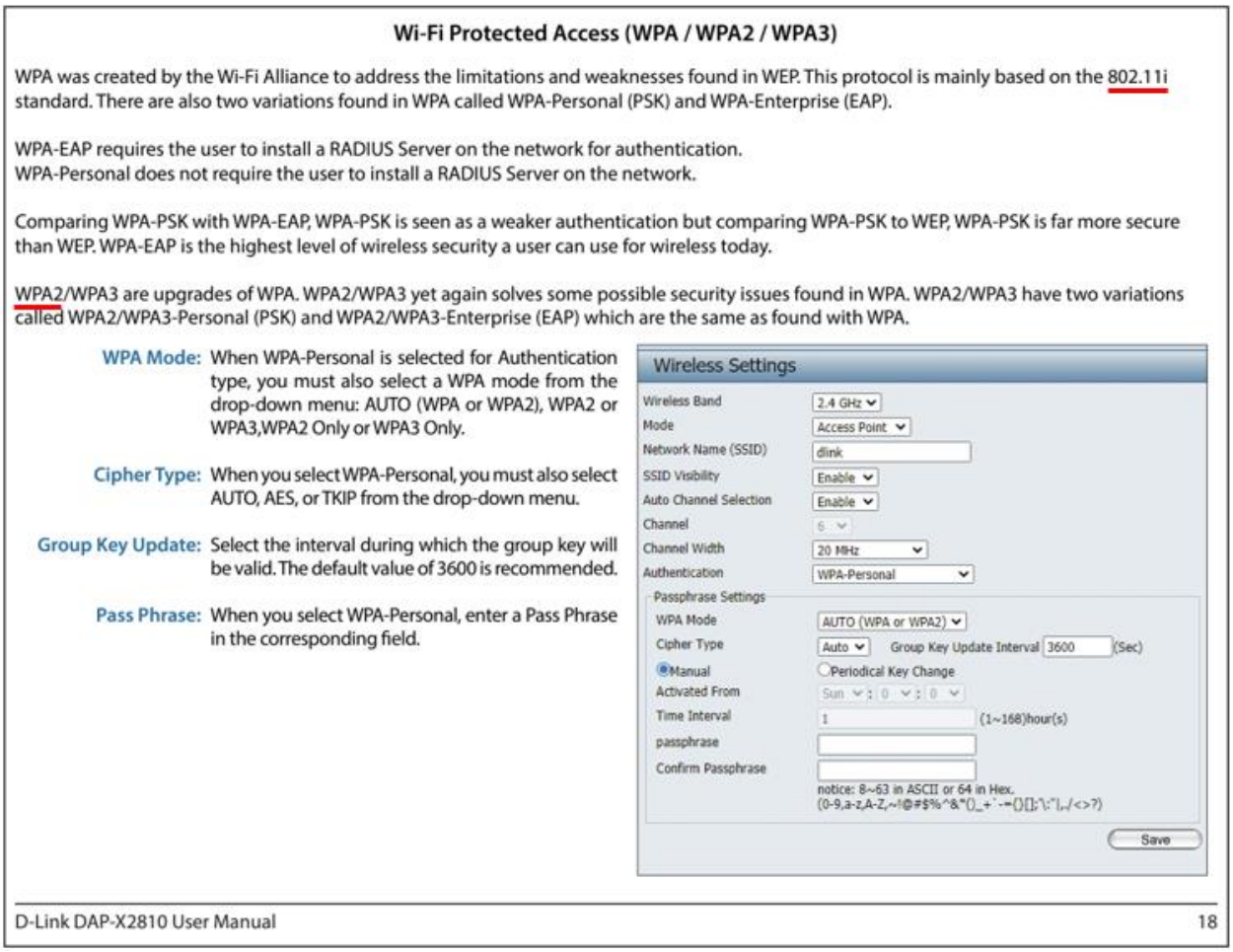




(*E.g.*, https://www.dlink.com/us/en/products/dap-x2810-ax1800-wifi-6-dualband-poe-access-point).

Functionality	
Standards	IEEE 802.11a/b/g/n/ac/ax, IEEE 802.3u/ab, IEEE 802.3az Energy-Efficient Ethernet (EEE), IEEE 802.3at PoE
Operating Frequency	2.4 - 2.483 GHz, 5.15 - 5.35 GHz, 5.47 - 5.85 GHz
Security Protocol	WPA/WPA2/WPA3™ Personal/Enterprise, WEP 64/128-bit, SSID broadcast disable, MAC address access control, internal RADIUS server

(*E.g.*, https://www.dlink.com/us/en/-/media/business_products/dap/dap-x2810/datasheet/dap_x2810_datasheet_eu_en.pdf).



Wi-Fi Protected Access (WPA / WPA2 / WPA3)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a RADIUS Server on the network for authentication.
WPA-Personal does not require the user to install a RADIUS Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

WPA2/WPA3 are upgrades of WPA. WPA2/WPA3 yet again solves some possible security issues found in WPA. WPA2/WPA3 have two variations called WPA2/WPA3-Personal (PSK) and WPA2/WPA3-Enterprise (EAP) which are the same as found with WPA.

WPA Mode: When WPA-Personal is selected for Authentication type, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 or WPA3,WPA2 Only or WPA3 Only.

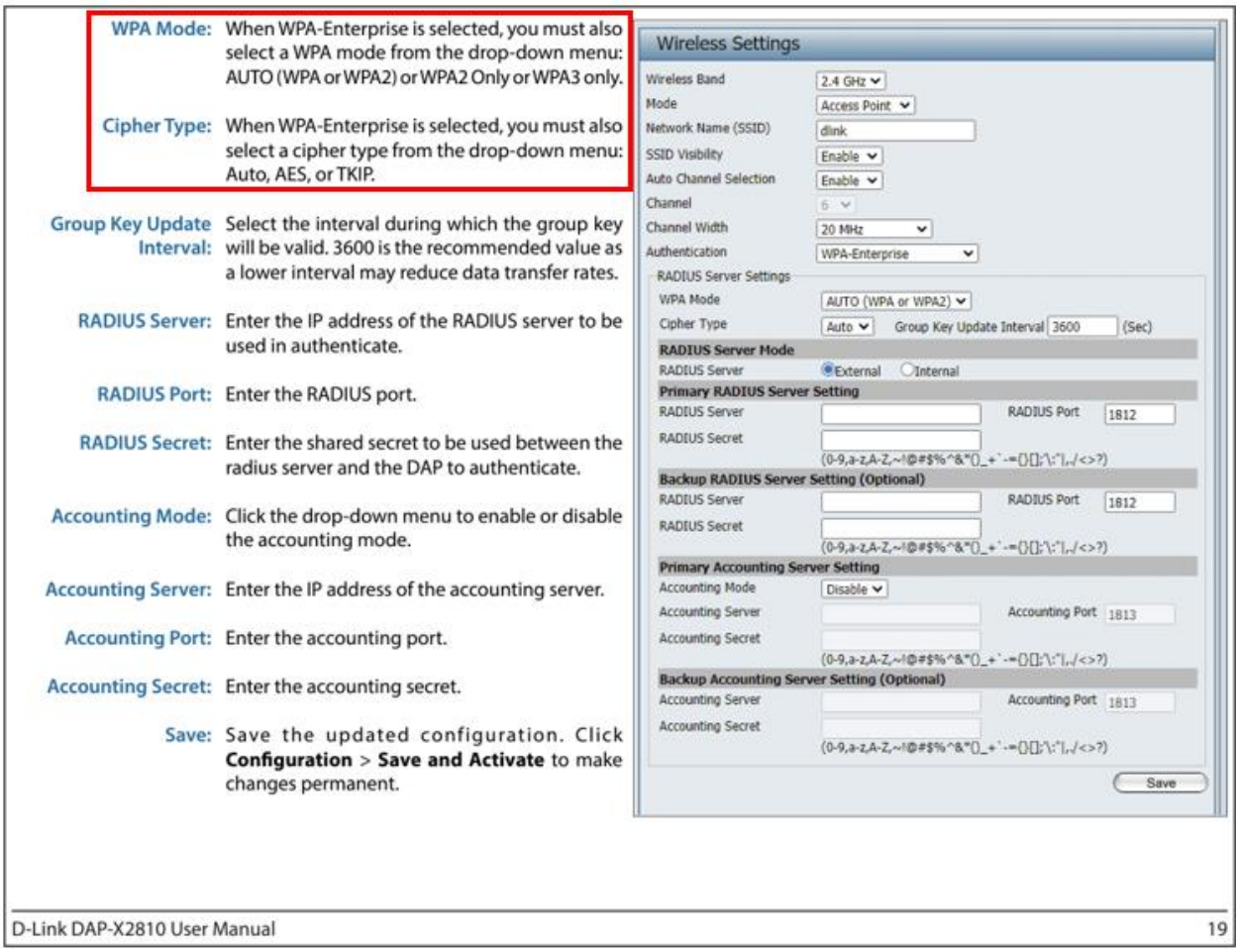
Cipher Type: When you select WPA-Personal, you must also select AUTO, AES, or TKIP from the drop-down menu.

Group Key Update: Select the interval during which the group key will be valid. The default value of 3600 is recommended.

Pass Phrase: When you select WPA-Personal, enter a Pass Phrase in the corresponding field.

D-Link DAP-X2810 User Manual 18

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).



WPA Mode: When WPA-Enterprise is selected, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2) or WPA2 Only or WPA3 only.

Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.

Group Key Update Interval: Select the interval during which the group key will be valid. 3600 is the recommended value as a lower interval may reduce data transfer rates.

RADIUS Server: Enter the IP address of the RADIUS server to be used in authenticate.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the shared secret to be used between the radius server and the DAP to authenticate.

Accounting Mode: Click the drop-down menu to enable or disable the accounting mode.

Accounting Server: Enter the IP address of the accounting server.

Accounting Port: Enter the accounting port.

Accounting Secret: Enter the accounting secret.

Save: Save the updated configuration. Click **Configuration** > **Save and Activate** to make changes permanent.

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).

So not surprisingly, along with an IP address (which is networks software), there's also a hardware address. Typically it is tied to a key connection device in your computer called the network interface card, or NIC. The NIC is essentially a computer circuit card that makes it possible for your computer to connect to a network.

An NIC turns data into an electrical signal that can be transmitted over the network.

Hey Nick. Meet Mac.

Every NIC has a hardware address that's known as a MAC, for Media Access Control. Where IP addresses are associated with TCP/IP (networking software), MAC addresses are linked to the hardware of network adapters.

A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it. Something called the ARP (Address Resolution Protocol) translates an IP address into a MAC address. The ARP is like a passport that takes data from an IP address through an actual piece of computer hardware.

(*E.g.*, https://whatismyipaddress.com/mac-address).

- 802.11 frames have up to four address fields in the MAC header.
- 802.11 frames typically use only three of the MAC address fields (4 in WDS environment).

Bytes	2	2	6	6	6	2	6	2
	Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	QoS control

Figure 9.3 802.11 MAC header

(*E.g.*, https://dot11ap.wordpress.com/ieee-802-11-frame-format-vs-ieee-802-3-frame-format/).

Depending on whether the 802.11 traffic is upstream or downstream, the definition of each of the four MAC address fields in the layer 2 header will change.

The five definitions are as follows:

- **Source Address (SA)** The MAC address of the original sending station is known as the SA. The source address can originate from either a wireless station or the wired network.
- **Destination Address (DA)** The MAC address that is the final destination of the layer 2 frame is known as the DA. The final destination may be a wireless station or could be a destination on the wired network such as a server or a router.

(*E.g.*, https://dot11ap.wordpress.com/ieee-802-11-frame-format-vs-ieee-802-3-frame-format/).

WPA-PSK

WPA-PSK uses this kind of key-encryption system to protect Wi-Fi networks. When you set a WPA-PSK password on the router, you are actually setting the key which the WPA standard will use to encrypt data. When users type in this matching key as their "password" their computers will be able to communicate with the router. Otherwise, they can't join the network because their computers will be incapable of understanding anything the router sends them. There is no such thing as a "default" key in key-based encryption methods. If your router is broadcasting with WPA-PSK, it means that someone with administrative access to the router enabled encryption with a key of his own choosing.

(*E.g.*, https://smallbusiness.chron.com/default-wpapsk-wifi-39458.html).

IEEE 802.11 defines two authentication methods: Open System authentication and Shared Key authentication. Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA also supports authentication based on IEEE 802.1X, or preshared keys (PSKs). IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This amendment does not specify an EAP method that is mandatory to implement. See 8.4.4 for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

In an RSNA, IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port.

(*E.g.*, IEEE 802.11i).

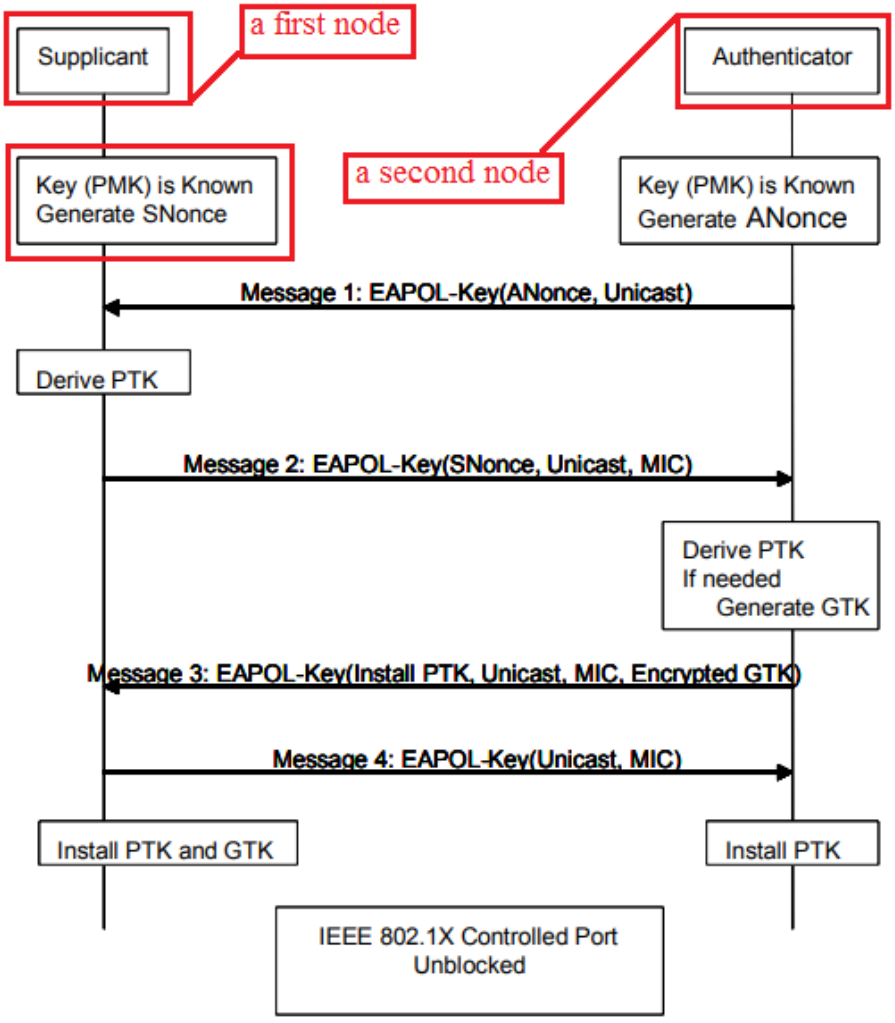
5.9.2.2 Operations with PSK

The following AKM operations are carried out when the PMK is a PSK:

— A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing (shown in Figure 11a). A STA associates with an AP and negotiates a security policy. The PMK is the PSK.

— The 4-Way Handshake using EAPOL-Key frames is used just as with IEEE 802.1X authentication, when an AS is present. See Figure 11c.

— The GTK and GTK sequence number are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 11c and Figure 11d.



(*E.g.*, IEEE 802.11i).

b) If an RSNA is based on a PSK in an ESS, the STA's SME establishes an RSNA as follows:

1) It identifies the AP as RSNA-capable from the AP's Beacon or Probe Response frames.

2) It shall invoke Open System authentication.

3) It negotiates cipher suites during the association process, as described in 8.4.2 and 8.4.3.

4) It establishes temporal keys by executing a key management algorithm, using the protocol defined by 8.5. It uses the PSK as the PMK.

5) It protects the data link by programming the negotiated cipher suites and the established temporal key into the MAC and then invoking protection.

c) If an RSNA is based on a PSK in an IBSS, the STA's SME executes the following sequence of procedures:

1) It identifies the peer as RSNA-capable from the peer's Beacon or Probe Response frames.

NOTE—STAs may respond to a data MPDU from an unrecognized STA by sending a Probe Request frame to find out whether the unrecognized STA is RSNA-capable.

2) It may optionally invoke Open System authentication.

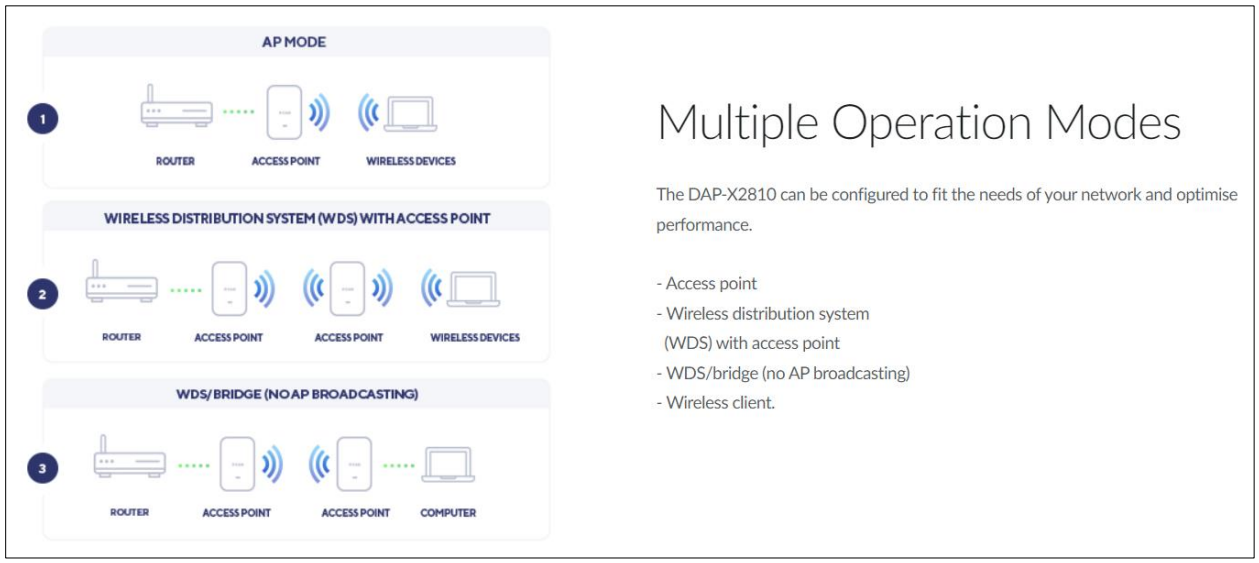
3) Each STA uses the procedures in 8.5, to establish temporal keys and to negotiate cipher suites. It uses a PSK as the PMK. Note that two peer STAs may follow this procedure simultaneously. See 8.4.9.

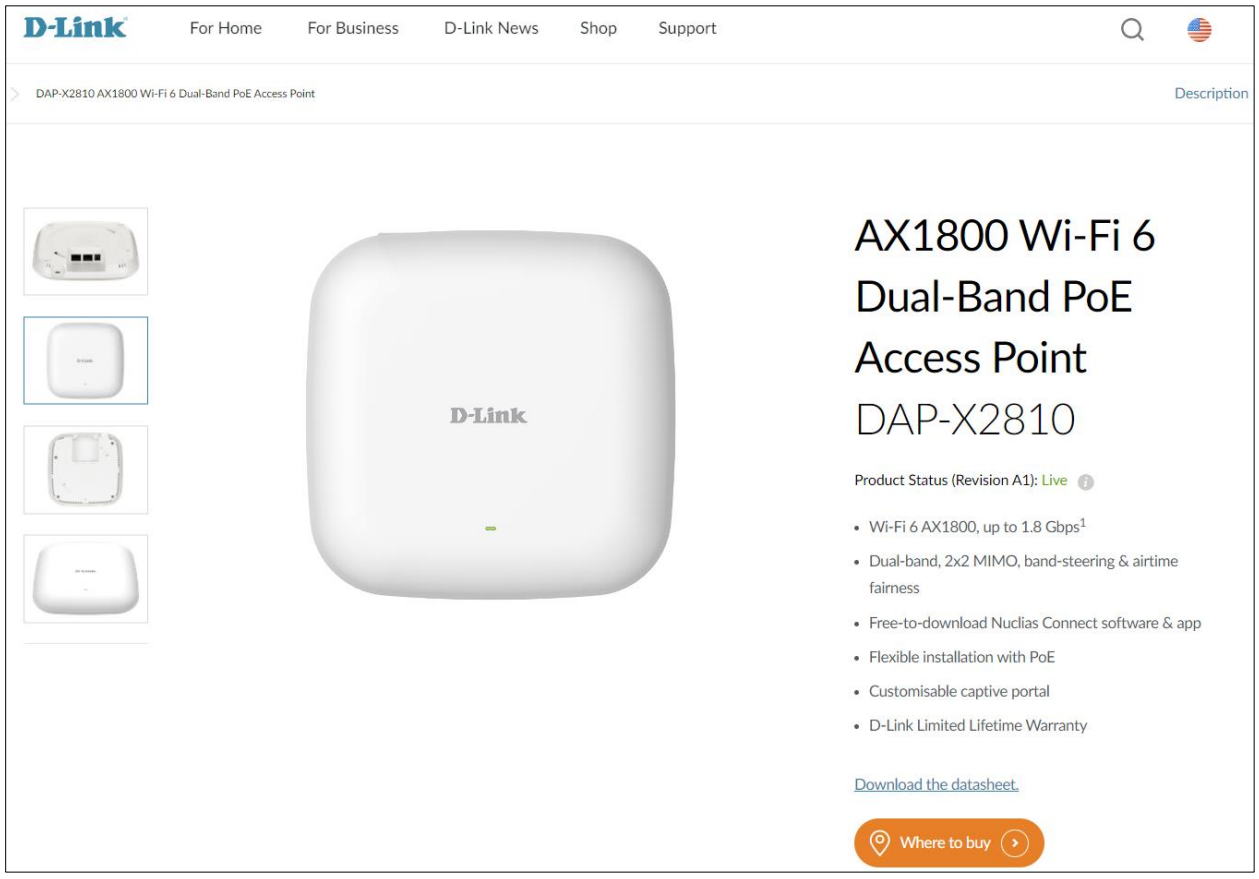
4) It protects the data link by programming the negotiated cipher suites and the established temporal key and then invoking protection.

(*E.g.*, IEEE 802.11i).

25. Upon information and belief, the system utilized by the Accused Instrumentality practices storing the node identifier (*e.g.*, MAC address of an accessory device and pre-shared key or pairwise master key) at a second network node (*e.g.*, the Accused Instrumentality). The Accused Instrumentality stores the MAC address of an accessory device and the pre-shared key or pairwise master key. To join the Wi-Fi network of the Accused Instrumentality, an accessory device transmits a response for a beacon transmitted by the Accused Instrumentality or sends a probe request to the Accused Instrumentality. A Wi-Fi header comprises the MAC address of a sender. The accessory device must send its MAC address. The Accused Instrumentality receives and stores the MAC address of the accessory device. Also, the Accused Instrumentality stores the Wi-Fi

password which is pre-shared key or pairwise master key (*e.g.*, initial authentication key) of its wireless personal network.





(*E.g.*, https://www.dlink.com/us/en/products/dap-x2810-ax1800-wifi-6-dualband-poe-access-point).

Functionality	
Standards	IEEE 802.11a/b/g/n/ac/ax, IEEE 802.3u/ab, IEEE 802.3az Energy-Efficient Ethernet (EEE), IEEE 802.3at PoE
Operating Frequency	2.4 - 2.483 GHz, 5.15 - 5.35 GHz, 5.47 - 5.85 GHz
Security Protocol	WPA/WPA2/WPA3™ Personal/Enterprise, WEP 64/128-bit, SSID broadcast disable, MAC address access control, internal RADIUS server

(*E.g.*, https://www.dlink.com/us/en/-/media/business_products/dap/dap-x2810/datasheet/dap_x2810_datasheet_eu_en.pdf).

Wi-Fi Protected Access (WPA / WPA2 / WPA3)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a RADIUS Server on the network for authentication.
WPA-Personal does not require the user to install a RADIUS Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

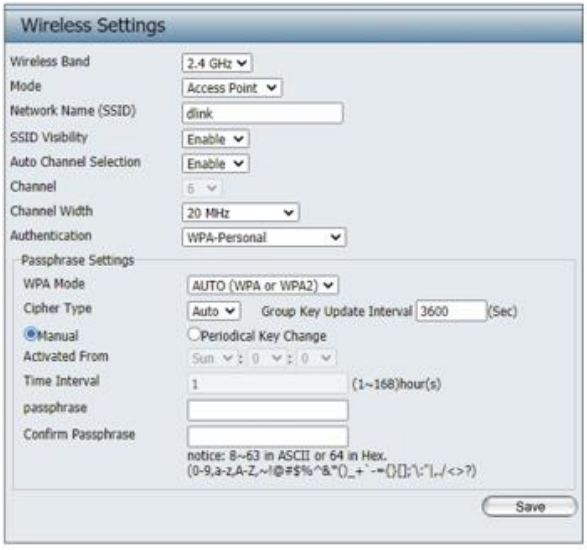
WPA2/WPA3 are upgrades of WPA. WPA2/WPA3 yet again solves some possible security issues found in WPA. WPA2/WPA3 have two variations called WPA2/WPA3-Personal (PSK) and WPA2/WPA3-Enterprise (EAP) which are the same as found with WPA.

WPA Mode: When WPA-Personal is selected for Authentication type, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 or WPA3,WPA2 Only or WPA3 Only.

Cipher Type: When you select WPA-Personal, you must also select AUTO, AES, or TKIP from the drop-down menu.

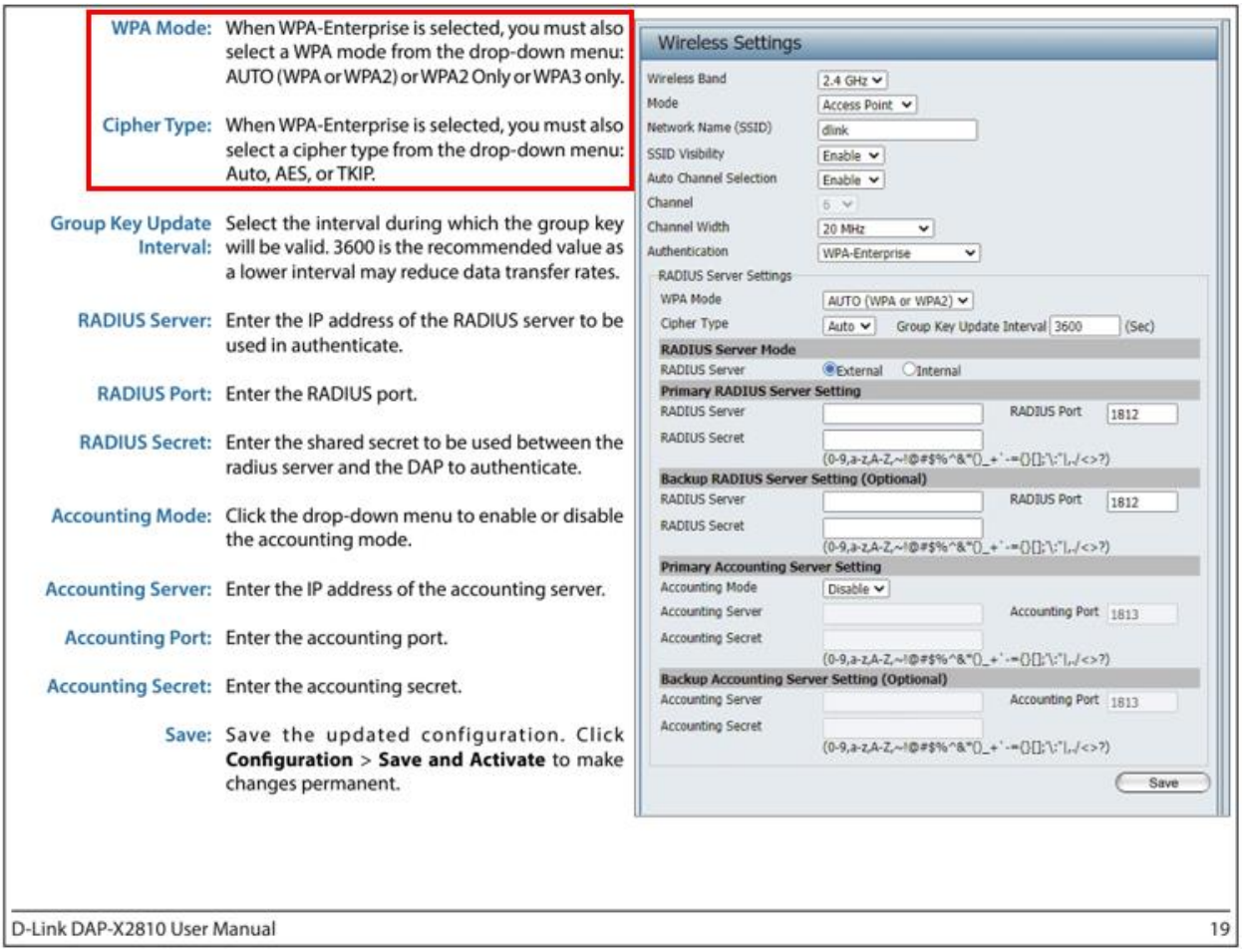
Group Key Update: Select the interval during which the group key will be valid. The default value of 3600 is recommended.

Pass Phrase: When you select WPA-Personal, enter a Pass Phrase in the corresponding field.



D-Link DAP-X2810 User Manual 18

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).



WPA Mode: When WPA-Enterprise is selected, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2) or WPA2 Only or WPA3 only.

Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.

Group Key Update Interval: Select the interval during which the group key will be valid. 3600 is the recommended value as a lower interval may reduce data transfer rates.

RADIUS Server: Enter the IP address of the RADIUS server to be used in authenticate.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the shared secret to be used between the radius server and the DAP to authenticate.

Accounting Mode: Click the drop-down menu to enable or disable the accounting mode.

Accounting Server: Enter the IP address of the accounting server.

Accounting Port: Enter the accounting port.

Accounting Secret: Enter the accounting secret.

Save: Save the updated configuration. Click **Configuration** > **Save and Activate** to make changes permanent.

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).

So not surprisingly, along with an IP address (which is networks software), there's also a hardware address. Typically it is tied to a key connection device in your computer called the network interface card, or NIC. The NIC is essentially a computer circuit card that makes it possible for your computer to connect to a network.

An NIC turns data into an electrical signal that can be transmitted over the network.

Hey Nick. Meet Mac.

Every NIC has a hardware address that's known as a MAC, for Media Access Control. Where IP addresses are associated with TCP/IP (networking software), MAC addresses are linked to the hardware of network adapters.

A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it. Something called the ARP (Address Resolution Protocol) translates an IP address into a MAC address. The ARP is like a passport that takes data from an IP address through an actual piece of computer hardware.

(*E.g.*, https://whatismyipaddress.com/mac-address).

5.9.2.2 Operations with PSK

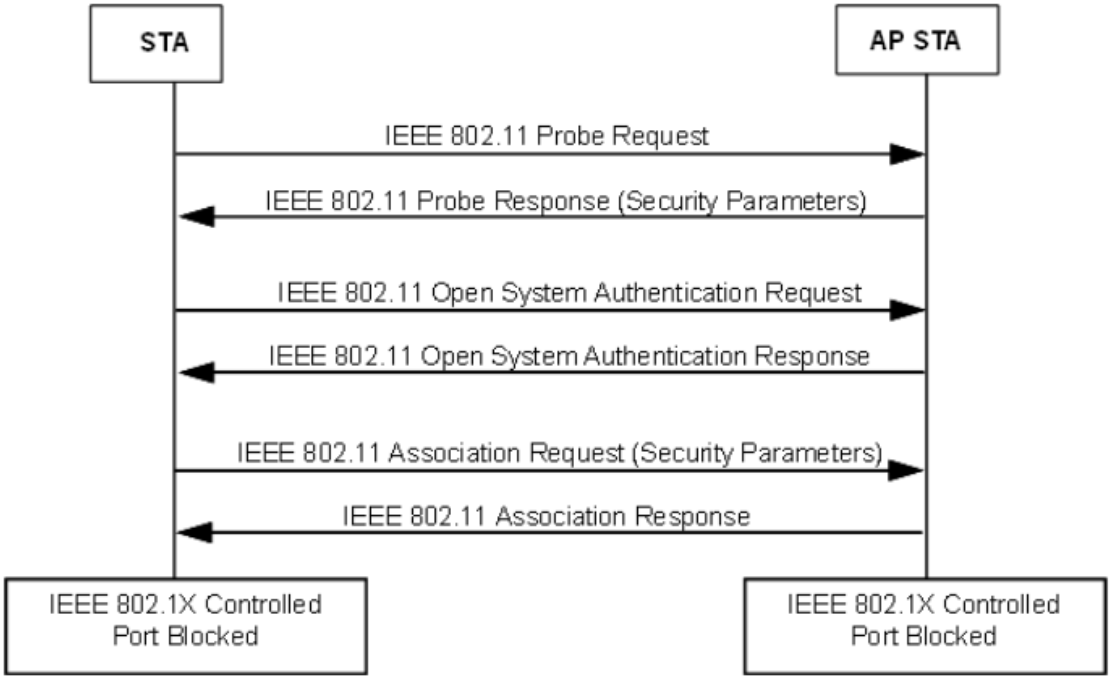
The following AKM operations are carried out when the PMK is a PSK:

— A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing (shown in Figure 11a). A STA associates with an AP and negotiates a security policy. The PMK is the PSK.

— The 4-Way Handshake using EAPOL-Key frames is used just as with IEEE 802.1X authentication, when an AS is present. See Figure 11c.

— The GTK and GTK sequence number are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 11c and Figure 11d.

(*E.g.*, IEEE 802.11i).



(*E.g.*, IEEE 802.11i).

- 802.11 frames have up to four address fields in the MAC header.
- 802.11 frames typically use only three of the MAC address fields (4 in WDS environment).

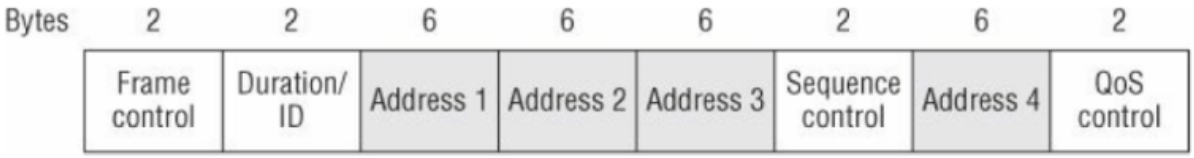


Figure 9.3 802.11 MAC header

(*E.g.*, https://dot11ap.wordpress.com/ieee-802-11-frame-format-vs-ieee-802-3-frame-format/).

Depending on whether the 802.11 traffic is upstream or downstream, the definition of each of the four MAC address fields in the layer 2 header will change.

The five definitions are as follows:

- **Source Address (SA)** The MAC address of the original sending station is known as the SA. The source address can originate from either a wireless station or the wired network.
- **Destination Address (DA)** The MAC address that is the final destination of the layer 2 frame is known as the DA. The final destination may be a wireless station or could be a destination on the wired network such as a server or a router.

(*E.g.*, https://dot11ap.wordpress.com/ieee-802-11-frame-format-vs-ieee-802-3-frame-format/).

WPA-PSK

WPA-PSK uses this kind of key-encryption system to protect Wi-Fi networks. When you set a WPA-PSK password on the router, you are actually setting the key which the WPA standard will use to encrypt data. When users type in this matching key as their "password" their computers will be able to communicate with the router. Otherwise, they can't join the network because their computers will be incapable of understanding anything the router sends them. There is no such thing as a "default" key in key-based encryption methods. If your router is broadcasting with WPA-PSK, it means that someone with administrative access to the router enabled encryption with a key of his own choosing.

(*E.g.*, https://smallbusiness.chron.com/default-wpapsk-wifi-39458.html).

IEEE 802.11 defines two authentication methods: Open System authentication and Shared Key authentication. Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA also supports authentication based on IEEE 802.1X, or preshared keys (PSKs). IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This amendment does not specify an EAP method that is mandatory to implement. See 8.4.4 for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

In an RSNA, IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port.

(*E.g.*, IEEE 802.11i).

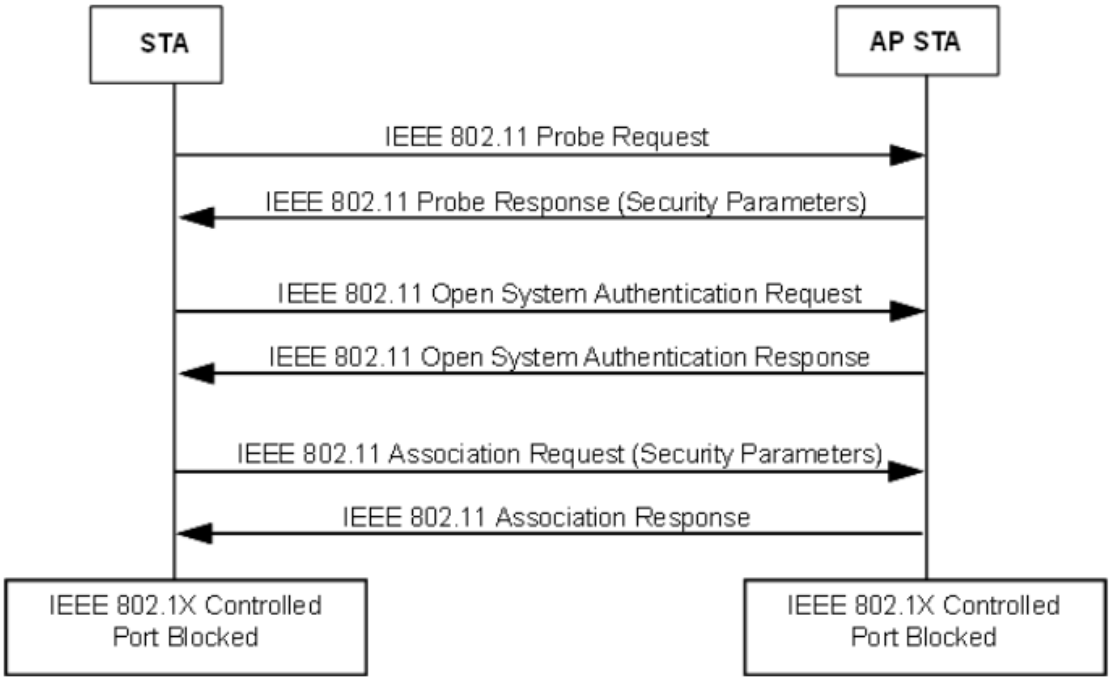
5.9.2.2 Operations with PSK

The following AKM operations are carried out when the PMK is a PSK:

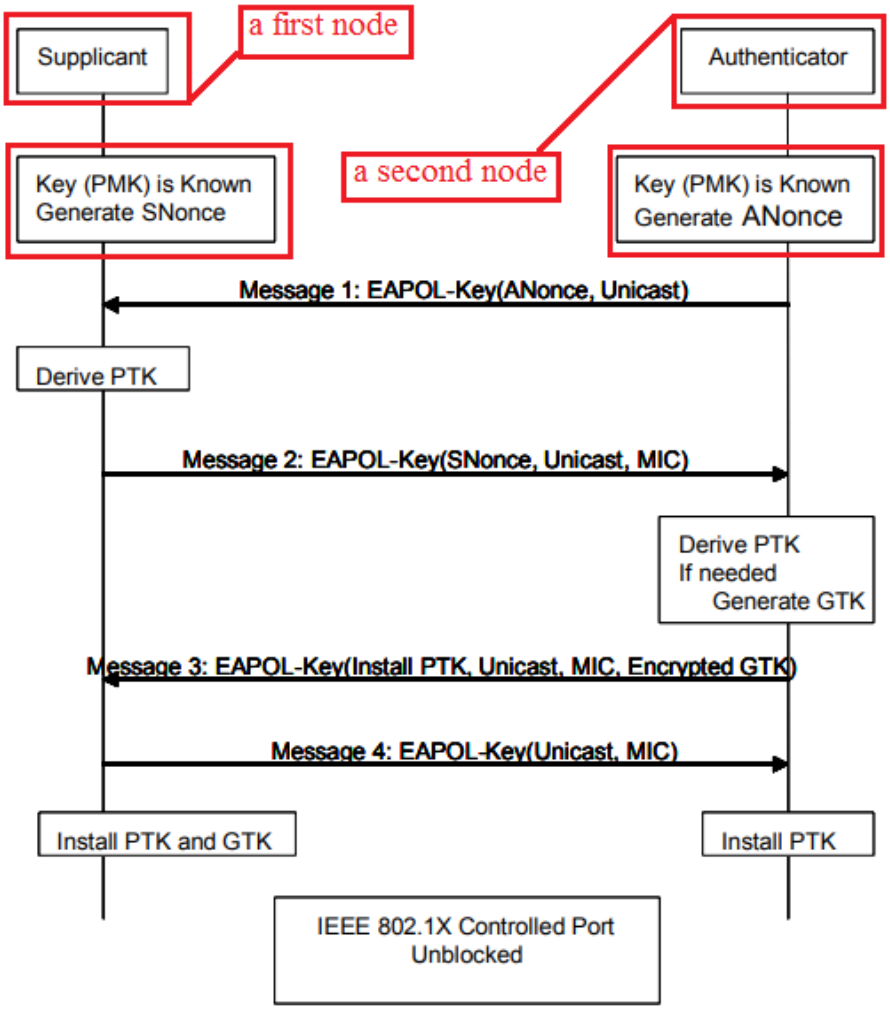
— A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing (shown in Figure 11a). A STA associates with an AP and negotiates a security policy. The PMK is the PSK.

— The 4-Way Handshake using EAPOL-Key frames is used just as with IEEE 802.1X authentication, when an AS is present. See Figure 11c.

— The GTK and GTK sequence number are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 11c and Figure 11d.



(*E.g.*, IEEE 802.11i).



(*E.g.*, IEEE 802.11i).

b) If an RSNA is based on a PSK in an ESS, the STA's SME establishes an RSNA as follows:

1) It identifies the AP as RSNA-capable from the AP's Beacon or Probe Response frames.

2) It shall invoke Open System authentication.

3) It negotiates cipher suites during the association process, as described in 8.4.2 and 8.4.3.

4) It establishes temporal keys by executing a key management algorithm, using the protocol defined by 8.5. It uses the PSK as the PMK.

5) It protects the data link by programming the negotiated cipher suites and the established temporal key into the MAC and then invoking protection.

c) If an RSNA is based on a PSK in an IBSS, the STA's SME executes the following sequence of procedures:

1) It identifies the peer as RSNA-capable from the peer's Beacon or Probe Response frames.

NOTE—STAs may respond to a data MPDU from an unrecognized STA by sending a Probe Request frame to find out whether the unrecognized STA is RSNA-capable.

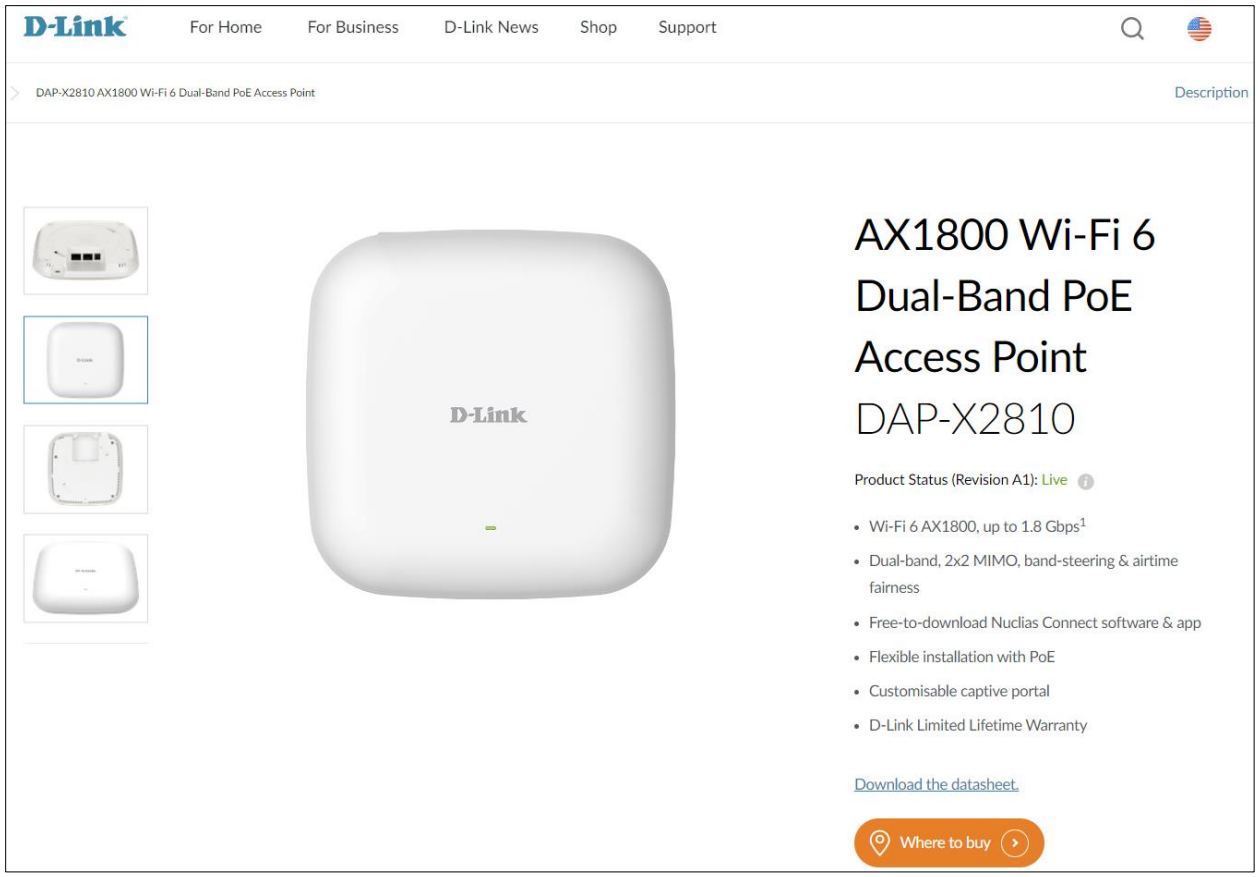
2) It may optionally invoke Open System authentication.

3) Each STA uses the procedures in 8.5, to establish temporal keys and to negotiate cipher suites. It uses a PSK as the PMK. Note that two peer STAs may follow this procedure simultaneously. See 8.4.9.

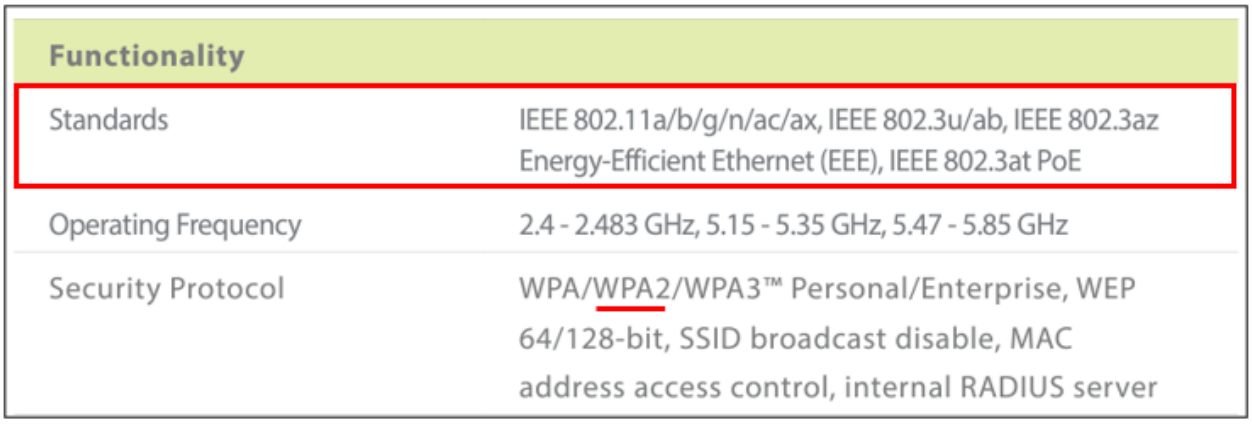
4) It protects the data link by programming the negotiated cipher suites and the established temporal key and then invoking protection.

(*E.g.*, IEEE 802.11i).

26. Upon information and belief, the system utilized by the Accused Instrumentality practices sending node identifier information (*e.g.*, MAC address of an accessory device and pre-shared key or pairwise master key) from a first network node (*e.g.*, an accessory device such as a Wi-Fi enabled smartphone, etc.) to a second network node (*e.g.*, the Accused Instrumentality). The accessory device sends its MAC address (*e.g.*, address) as well as a key value derived from the pre-shared key or pairwise master key (*e.g.*, initial authentication key) to the Accused Instrumentality for authentication to connect to Wi-Fi network of the Accused Instrumentality. A pairwise temporal key is derived from the pre-shared key or pairwise master key (*e.g.*, initial authentication key). The pairwise temporal key has two parts KCK and KEK. In the authentication process, the accessory device acts as a supplicant. As shown below, the accessory device transfers a key value derived from KCK in the EAPOL-message 2 to the Accused Instrumentality.

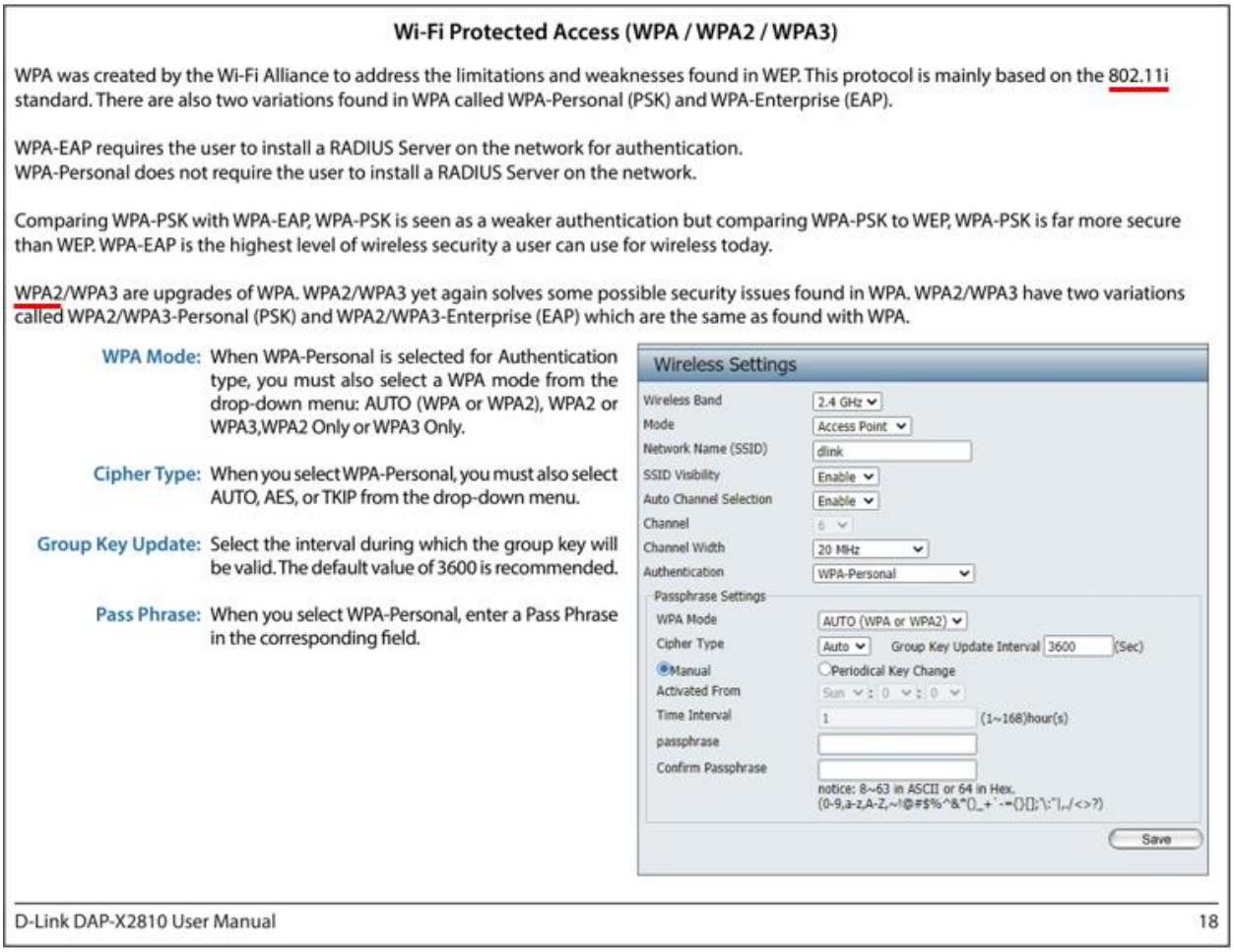


(*E.g.*, https://www.dlink.com/us/en/products/dap-x2810-ax1800-wifi-6-dualband-poe-access-point).



Functionality	
Standards	IEEE 802.11a/b/g/n/ac/ax, IEEE 802.3u/ab, IEEE 802.3az Energy-Efficient Ethernet (EEE), IEEE 802.3at PoE
Operating Frequency	2.4 - 2.483 GHz, 5.15 - 5.35 GHz, 5.47 - 5.85 GHz
Security Protocol	WPA/WPA2/WPA3™ Personal/Enterprise, WEP 64/128-bit, SSID broadcast disable, MAC address access control, internal RADIUS server

(*E.g.*, https://www.dlink.com/us/en/-/media/business_products/dap/dap-x2810/datasheet/dap_x2810_datasheet_eu_en.pdf).



Wi-Fi Protected Access (WPA / WPA2 / WPA3)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a RADIUS Server on the network for authentication.
WPA-Personal does not require the user to install a RADIUS Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

WPA2/WPA3 are upgrades of WPA. WPA2/WPA3 yet again solves some possible security issues found in WPA. WPA2/WPA3 have two variations called WPA2/WPA3-Personal (PSK) and WPA2/WPA3-Enterprise (EAP) which are the same as found with WPA.

WPA Mode: When WPA-Personal is selected for Authentication type, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 or WPA3,WPA2 Only or WPA3 Only.

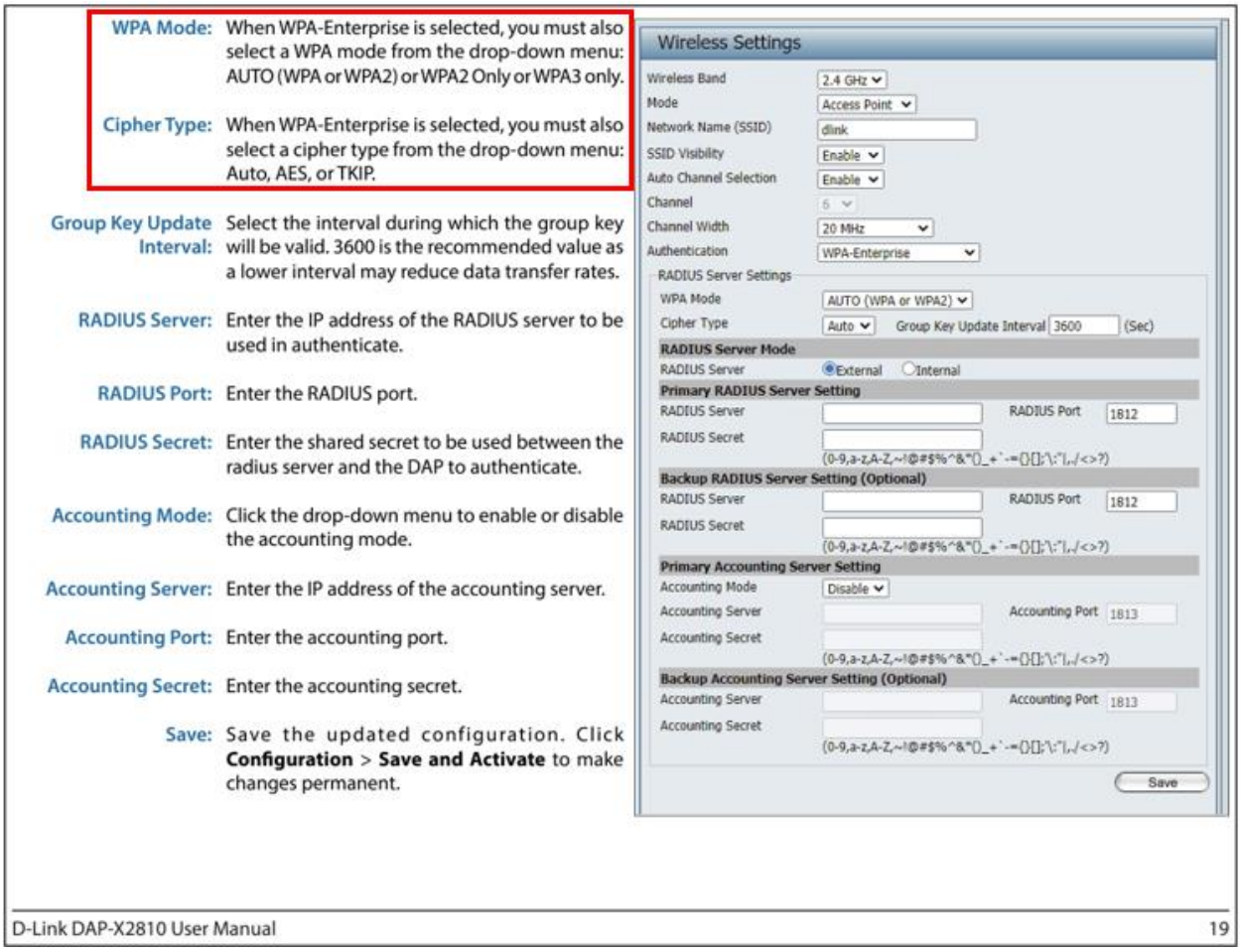
Cipher Type: When you select WPA-Personal, you must also select AUTO, AES, or TKIP from the drop-down menu.

Group Key Update: Select the interval during which the group key will be valid. The default value of 3600 is recommended.

Pass Phrase: When you select WPA-Personal, enter a Pass Phrase in the corresponding field.

D-Link DAP-X2810 User Manual 18

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).



WPA Mode: When WPA-Enterprise is selected, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2) or WPA2 Only or WPA3 only.

Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.

Group Key Update Interval: Select the interval during which the group key will be valid. 3600 is the recommended value as a lower interval may reduce data transfer rates.

RADIUS Server: Enter the IP address of the RADIUS server to be used in authenticate.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the shared secret to be used between the radius server and the DAP to authenticate.

Accounting Mode: Click the drop-down menu to enable or disable the accounting mode.

Accounting Server: Enter the IP address of the accounting server.

Accounting Port: Enter the accounting port.

Accounting Secret: Enter the accounting secret.

Save: Save the updated configuration. Click **Configuration** > **Save and Activate** to make changes permanent.

D-Link DAP-X2810 User Manual 19

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).

IEEE 802.11 defines two authentication methods: Open System authentication and Shared Key authentication. Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA also supports authentication based on IEEE 802.1X, or preshared keys (PSKs). IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This amendment does not specify an EAP method that is mandatory to implement. See 8.4.4 for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

In an RSNA, IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port.

5.9.2.2 Operations with PSK

The following AKM operations are carried out when the PMK is a PSK:

— A STA discovers the AP's security policy through passively monitoring Beacon frames or through active probing (shown in Figure 11a). A STA associates with an AP and negotiates a security policy. The PMK is the PSK.

— The 4-Way Handshake using EAPOL-Key frames is used just as with IEEE 802.1X authentication, when an AS is present. See Figure 11c.

— The GTK and GTK sequence number are sent from the Authenticator to the Supplicant just as in the AS case. See Figure 11c and Figure 11d.

(*E.g.*, IEEE 802.11i).

b) If an RSNA is based on a PSK in an ESS, the STA's SME establishes an RSNA as follows:

1) It identifies the AP as RSNA-capable from the AP's Beacon or Probe Response frames.

2) It shall invoke Open System authentication.

3) It negotiates cipher suites during the association process, as described in 8.4.2 and 8.4.3.

4) It establishes temporal keys by executing a key management algorithm, using the protocol defined by 8.5. It uses the PSK as the PMK.

5) It protects the data link by programming the negotiated cipher suites and the established temporal key into the MAC and then invoking protection.

c) If an RSNA is based on a PSK in an IBSS, the STA's SME executes the following sequence of procedures:

1) It identifies the peer as RSNA-capable from the peer's Beacon or Probe Response frames.

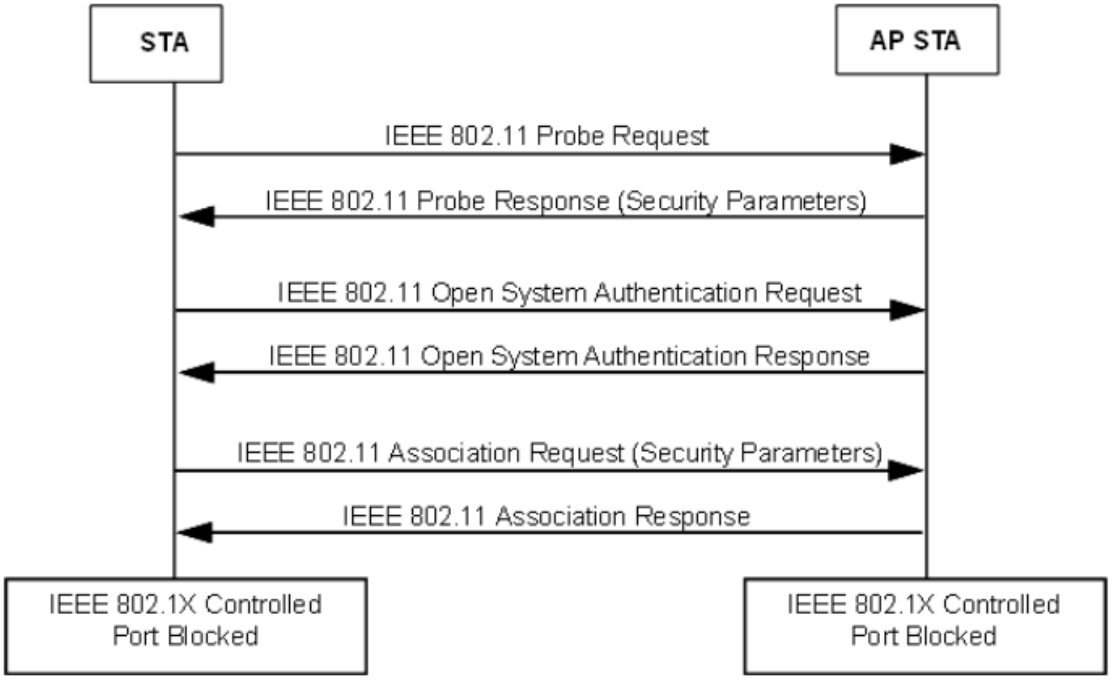
NOTE—STAs may respond to a data MPDU from an unrecognized STA by sending a Probe Request frame to find out whether the unrecognized STA is RSNA-capable.

2) It may optionally invoke Open System authentication.

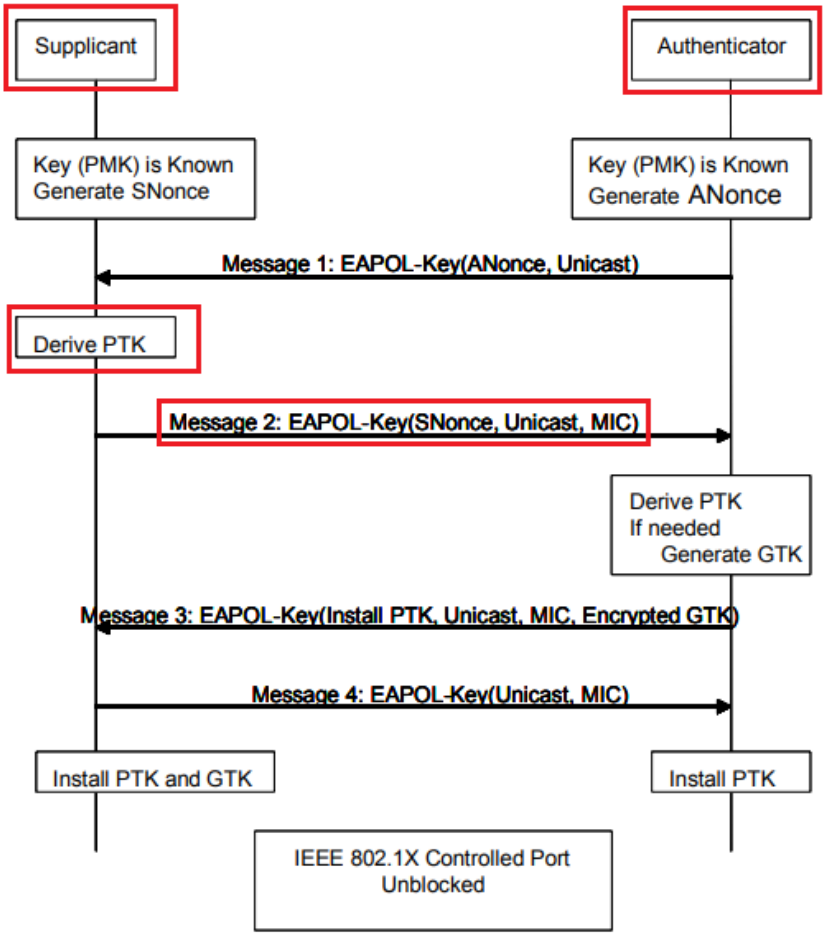
3) Each STA uses the procedures in 8.5, to establish temporal keys and to negotiate cipher suites. It uses a PSK as the PMK. Note that two peer STAs may follow this procedure simultaneously. See 8.4.9.

4) It protects the data link by programming the negotiated cipher suites and the established temporal key and then invoking protection.

(*E.g.*, IEEE 802.11i).



(*E.g.*, IEEE 802.11i).



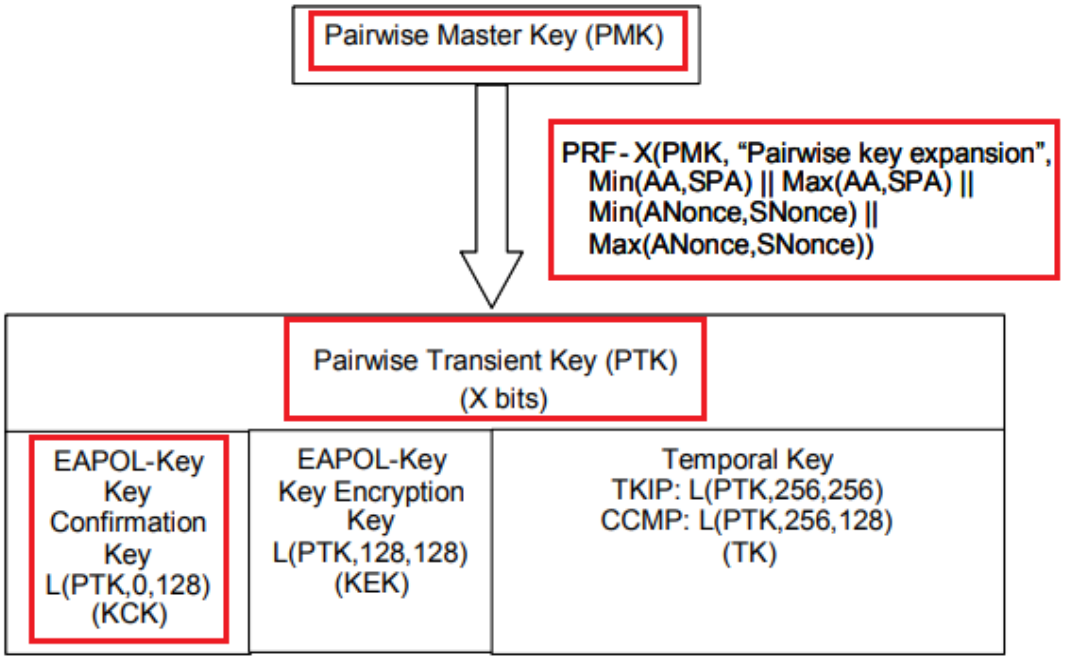
Descriptor Type – 1 octet	
Key Information – 2 octets	Key Length – 2 octets
Key Replay Counter – 8 octets	
Key Nonce – 32 octets	
EAPOL-Key IV – 16 octets	
Key RSC – 8 octets	
Reserved - 8 octets	
Key MIC – 16 octets	
Key Data Length – 2 octets	Key Data – n octets

Figure 43u—EAPOL-Key frame

(*E.g.*, IEEE 802.11i).

3.97 pairwise transient key (PTK): A value that is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Anthenticator nonce (ANonce), and Supplicant nonce (SNonce) using the pseudo-random function (PRF) and that is split up into as many as five keys, i.e., temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), EAPOL-Key confirmation key (KCK).

The pairwise key hierarchy utilizes PRF-384 or PRF-512 to derive session-specific keys from a PMK, as depicted in Figure 43s. The PMK shall be 256 bits. The pairwise key hierarchy takes a PMK and generates a PTK. The PTK is partitioned into KCK and KEK, and temporal keys used by the MAC to protect unicast communication between the Authenticator's and Supplicant's respective STAs. PTKs are used between a single Supplicant and a single Authenticator.



3.117 Supplicant address (SPA): The Supplicant's medium access control (MAC) address.

(*E.g.*, IEEE 802.11i).

8.5.3.2 4-Way Handshake Message 2

Message 2 uses the following values for each of the EAPOL-Key frame fields:

Descriptor Type = N – see 8.5.2

Key Information:

Key Descriptor Version = 1 (RC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA1-128) – same as Message 1

Key Type = 1 (Pairwise) – same as Message 1

Install = 0

Key Ack = 0

Key MIC = 1

Secure = 0 – same as Message 1

Error = 0 – same as Message 1

Request = 0 – same as Message 1

Encrypted Key Data = 0

Reserved = 0 – unused by this protocol version

Key Length = 0

Key Replay Counter = *n* – to let the Authenticator know to which Message 1 this corresponds

Key Nonce = SNonce

EAPOL-Key IV = 0

Key RSC = 0

Key MIC = MIC(KCK, EAPOL) – MIC computed over the body of this EAPOL-Key frame with the Key MIC field first initialized to 0

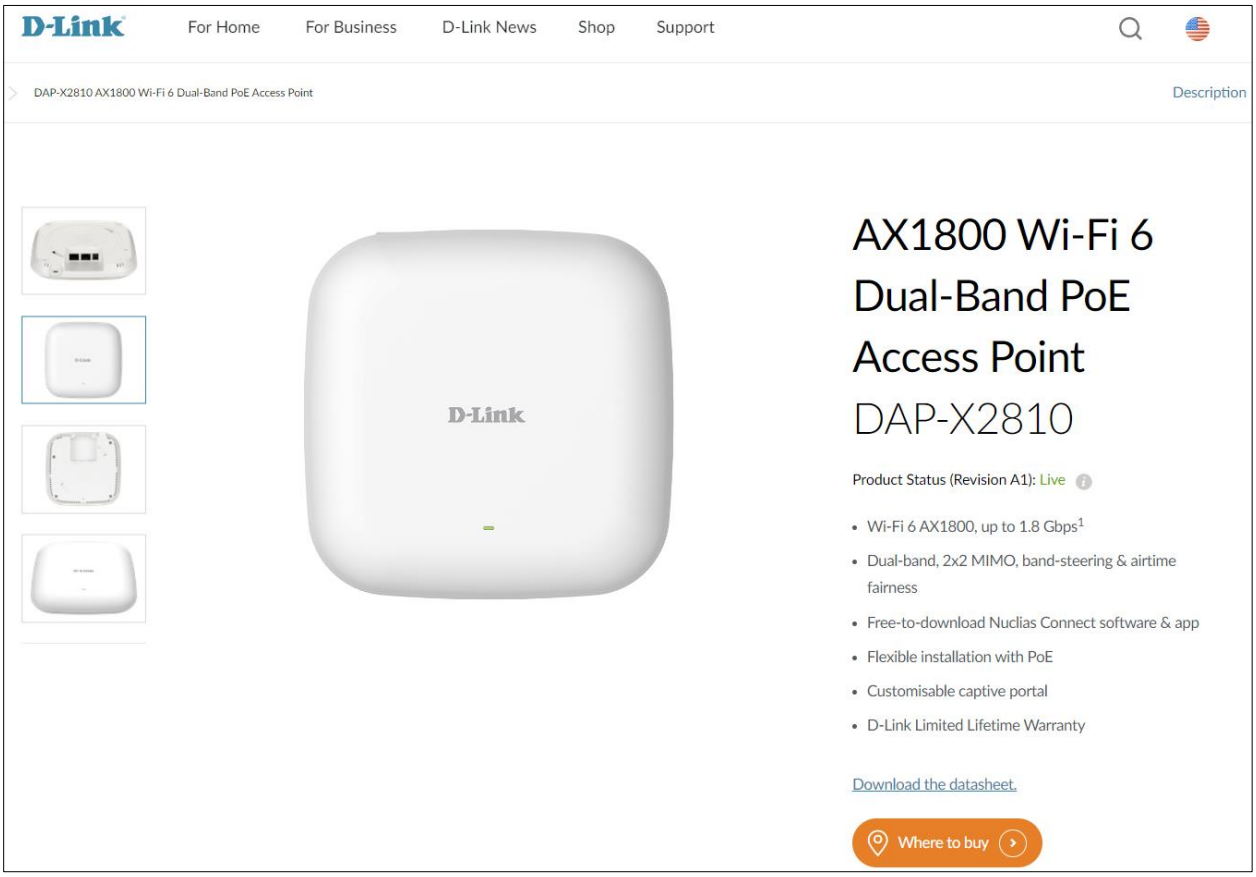
Key Data Length = length in octets of included RSN information element

Key Data = included RSN information element – the sending STA's RSN information element

(*E.g.*, IEEE 802.11i).

27. Upon information and belief, the system utilized by the Accused Instrumentality practices synchronously regenerating an authentication key (*e.g.*, temporal keys) at two network nodes (*e.g.*, the Accused Instrumentality and an accessory device such as a Wi-Fi enabled smartphone, etc.) based upon node identifier information. As shown below, the accessory device sends its MAC address (*e.g.*, address) as well as a key value derived from the pre-shared key or pairwise master key (*e.g.*, initial authentication key) to the Accused Instrumentality for authentication prior to connecting to the Wi-Fi network of the Accused Instrumentality. The Accused Instrumentality and the accessory device both regenerate temporal keys each time the devices get connected to each other. The Accused Instrumentality and the accessory device, both

synchronously install temporal keys (*i.e.*, a pairwise temporal key) with the help of a 4-way handshake message transfer having the node identifier information for establishing secured wireless communication.



(*E.g.*, https://www.dlink.com/us/en/products/dap-x2810-ax1800-wifi-6-dualband-poe-access-point).

Functionality	
Standards	IEEE 802.11a/b/g/n/ac/ax, IEEE 802.3u/ab, IEEE 802.3az Energy-Efficient Ethernet (EEE), IEEE 802.3at PoE
Operating Frequency	2.4 - 2.483 GHz, 5.15 - 5.35 GHz, 5.47 - 5.85 GHz
Security Protocol	WPA/WPA2/WPA3™ Personal/Enterprise, WEP 64/128-bit, SSID broadcast disable, MAC address access control, internal RADIUS server

(*E.g.*, https://www.dlink.com/us/en/-/media/business_products/dap/dap-x2810/datasheet/dap_x2810_datasheet_eu_en.pdf).

Wi-Fi Protected Access (WPA / WPA2 / WPA3)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a RADIUS Server on the network for authentication.
WPA-Personal does not require the user to install a RADIUS Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

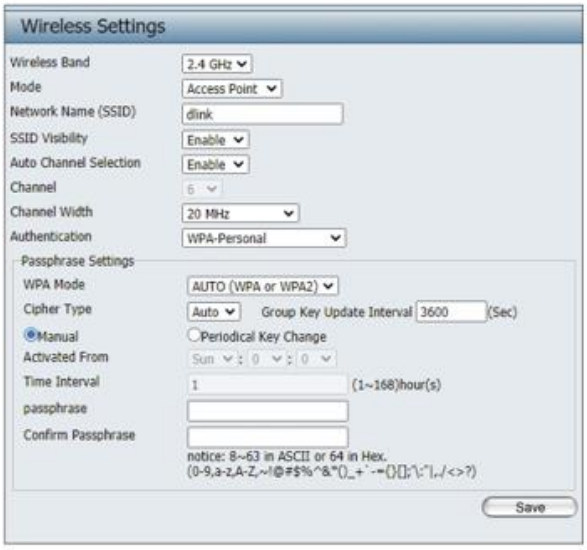
WPA2/WPA3 are upgrades of WPA. WPA2/WPA3 yet again solves some possible security issues found in WPA. WPA2/WPA3 have two variations called WPA2/WPA3-Personal (PSK) and WPA2/WPA3-Enterprise (EAP) which are the same as found with WPA.

WPA Mode: When WPA-Personal is selected for Authentication type, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 or WPA3,WPA2 Only or WPA3 Only.

Cipher Type: When you select WPA-Personal, you must also select AUTO, AES, or TKIP from the drop-down menu.

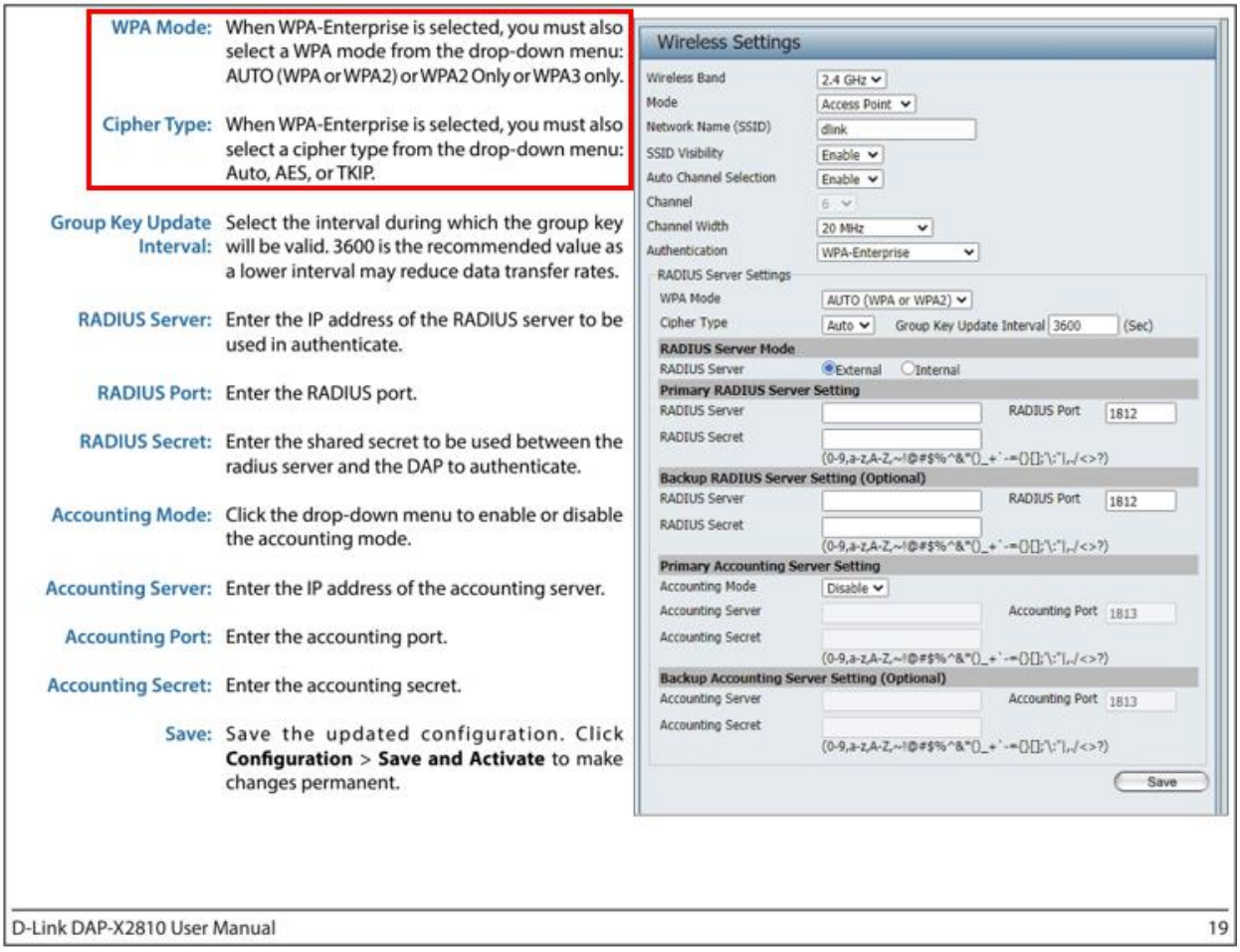
Group Key Update: Select the interval during which the group key will be valid. The default value of 3600 is recommended.

Pass Phrase: When you select WPA-Personal, enter a Pass Phrase in the corresponding field.



D-Link DAP-X2810 User Manual 18

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).



WPA Mode: When WPA-Enterprise is selected, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2) or WPA2 Only or WPA3 only.

Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.

Group Key Update Interval: Select the interval during which the group key will be valid. 3600 is the recommended value as a lower interval may reduce data transfer rates.

RADIUS Server: Enter the IP address of the RADIUS server to be used in authenticate.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the shared secret to be used between the radius server and the DAP to authenticate.

Accounting Mode: Click the drop-down menu to enable or disable the accounting mode.

Accounting Server: Enter the IP address of the accounting server.

Accounting Port: Enter the accounting port.

Accounting Secret: Enter the accounting secret.

Save: Save the updated configuration. Click **Configuration** > **Save and Activate** to make changes permanent.

D-Link DAP-X2810 User Manual 19

(*E.g.*, https://media.dlink.eu/support/products/dap/dap-x2810/documentation/dap-x2810_man_reva1_1-00_eu_multi_20211012.pdf).

8.4.8 RSNA key management in an ESS

When the IEEE 802.1X authentication completes successfully, this amendment assumes that the STA's IEEE 802.1X Supplicant and the IEEE 802.1X AS will share a secret, called a PMK. The AS transfers the PMK, within the AAA key, to the AP, using a technique that is outside the scope of this amendment; the derivation of the PMK from the MSK is EAP-method-specific. With the PMK in place, the AP initiates a key confirmation handshake with the STA. The key confirmation handshake sets the IEEE 802.1X state variable portValid (as described in IEEE P802.1X-REV) to TRUE.

The key confirmation handshake is implemented by the 4-Way Handshake. The purposes of the 4-Way Handshake are as follows:

a) Confirm the existence of the PMK at the peer.
b) Ensure that the security association keys are fresh.
c) Synchronize the installation of temporal keys into the MAC.
d) Transfer the GTK from the Authenticator to the Supplicant.

(*E.g.*, IEEE 802.11i).

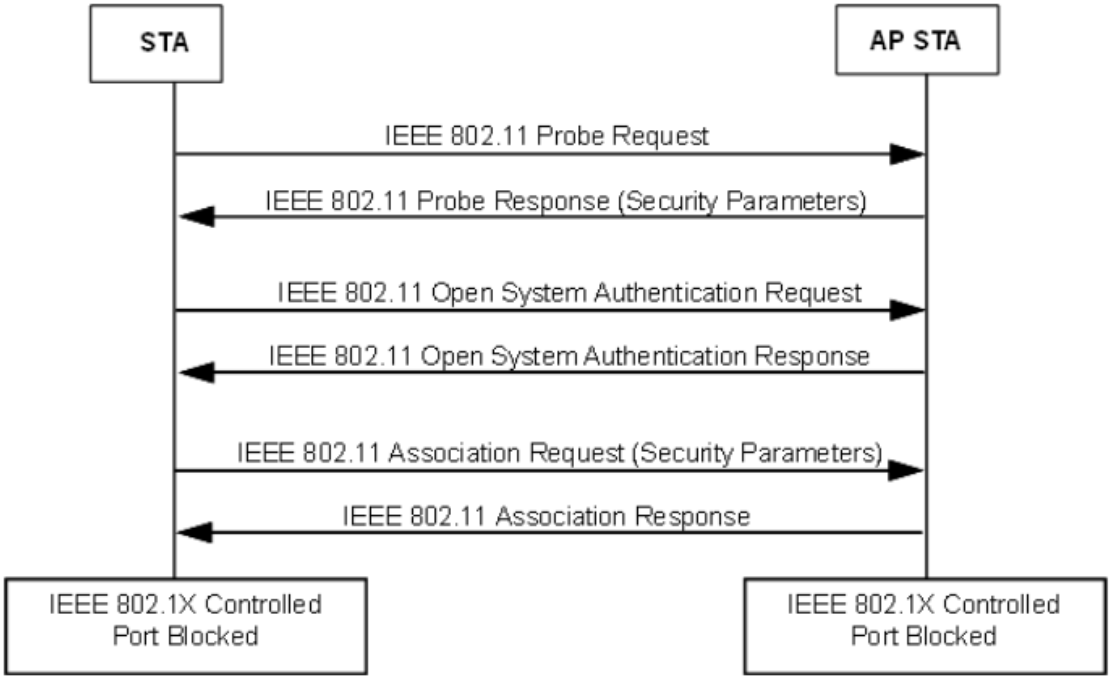
These are referred to as the temporal keys because they are recomputed every time a mobile device associates to the access point. The collection of all four keys together is referred to as the pairwise transient key (PTK). For RSN/TKIP and WPA, each of these keys must be 128 bits long so that the PTK is a total of 512 bits long.

The first two temporal keys sound familiar. They are the ones used to encrypt the data and protect it from modification. The second two we have not seen before. These are used to protect the communications between the access point and mobile device during the initial handshake.[2] For the moment, just accept that these EAPOL keys are needed; we will discuss them again shortly.

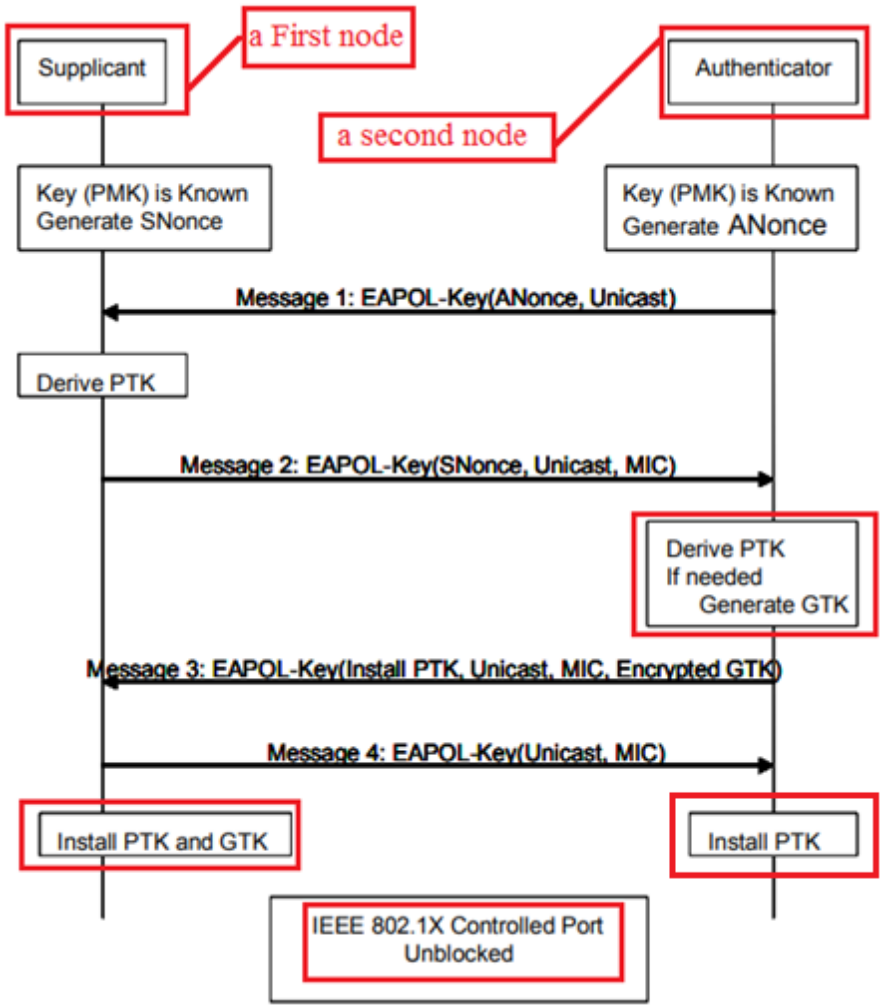
> [2] And for various notifications after the handshake.

Because the temporal keys are recomputed each time a mobile device connects, there has to be something that changes when the computation is done; otherwise, you'd end up with the same temporal keys every time. This is called adding liveness to the keys, ensuring that old keys no longer work. Liveness is achieved by including a couple of special values called nonces in the computation. The value of the nonce is quite arbitrary except in one respect: a nonce value is never used twice[3] with the same key. The word "nonce" can be thought of as "N ? once"?in other words, a value (N) only used once.[4] They say lightning never strikes in the same place twice (which is not true) and similarly nonces never come up with the same value twice (which should be true by design).

(*E.g.*, http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+10.+WPA+and+RSN+Key+Hierarchy/Pairwise+Key+Hierarchy/).



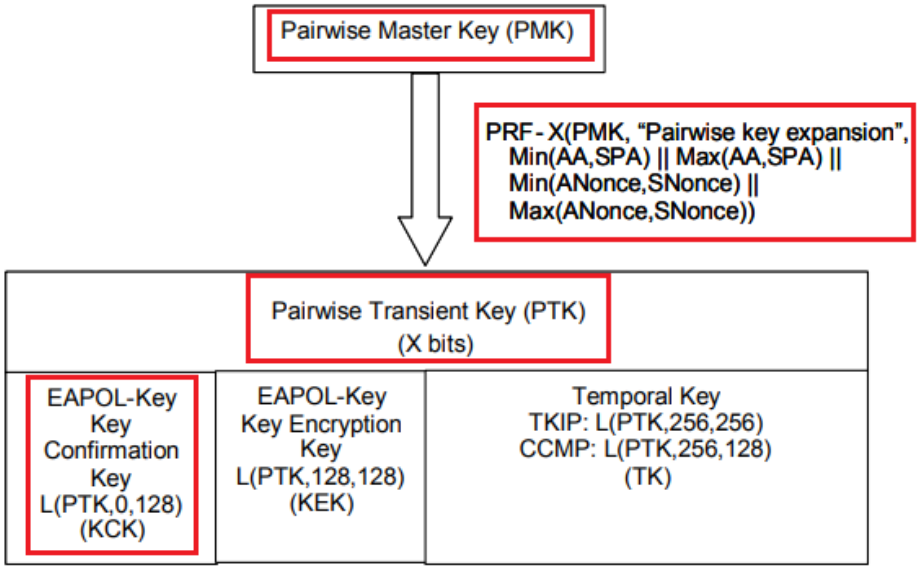
(*E.g.*, IEEE 802.11i).



3.97 pairwise transient key (PTK): A value that is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Anthenticator nonce (ANonce), and Supplicant nonce (SNonce) using the pseudo-random function (PRF) and that is split up into as many as five keys, i.e., temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), EAPOL-Key confirmation key (KCK).

(*E.g.*, IEEE 802.11i).

The pairwise key hierarchy utilizes PRF-384 or PRF-512 to derive session-specific keys from a PMK, as depicted in Figure 43s. The PMK shall be 256 bits. The pairwise key hierarchy takes a PMK and generates a PTK. The PTK is partitioned into KCK and KEK, and temporal keys used by the MAC to protect unicast communication between the Authenticator's and Supplicant's respective STAs. PTKs are used between a single Supplicant and a single Authenticator.



(*E.g.*, IEEE 802.11i).

28. Defendant's customers also infringe claim 1 of the '664 patent by using or performing the claimed method using the Accused Instrumentality as described above. Furthermore, Defendant advertises, markets, and offers for sale the Accused Instrumentality to its customers for use in a system in a manner that, as described above, infringes claim 1 of the '664 patent. Exemplary advertising and marketing material is cited above.

29. Plaintiff has been damaged as a result of Defendant's infringing conduct. Defendant is thus liable to Plaintiff for damages in an amount that adequately compensates Plaintiff for such Defendant's infringement of the '664 patent, *i.e.*, in an amount that by law cannot be less than would constitute a reasonable royalty for the use of the patented technology, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

30. On information and belief, Defendant has had at least constructive notice of the '664 patent by operation of law and, to the extent required, marking requirements have been complied with.

31. On information and belief, Defendant will continue its infringement of one or more claims of the '664 patent unless enjoined by the Court. Defendant's infringing conduct thus causes Plaintiff irreparable harm and will continue to cause such harm without the issuance of an injunction.

IV. JURY DEMAND

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

a. Judgment that one or more claims of United States Patent No. 7,233,664 have been infringed, either literally and/or under the doctrine of equivalents, by Defendant;

b. Judgment that Defendant account for and pay to Plaintiff all damages to and costs incurred by Plaintiff because of Defendant's infringing activities and other conduct complained of herein;

c. That Defendant be enjoined from future infringing activities;

d. That Plaintiff be granted pre-judgment and post-judgment interest on the damages caused by Defendant's infringing activities and other conduct complained of herein; and

e. That Plaintiff be granted such other and further relief as the Court may deem just and proper under the circumstances.

March 22, 2024

DIRECTION IP LAW

/s/ David R. Bennett

David R. Bennett
Direction IP Law
P.O. Box 14184
Chicago, IL 60614-0184
(312) 291-1667
dbennett@directionip.com

Attorneys for Plaintiff Encryptawave Technologies LLC