NXC5500/2500

Version 4.20
Edition 2, 02/2015

Application Note

802.11w Management Frame Protection

802.11w

Management Frame Protection

Introduction

IEEE 802.11w is the Management Frames Protection (MFP) standard for the IEEE 802.11 family of standards. IEEE 802.11w provides protection for management frames, extending the encryption and authentication methods defined in 802.11i to cover these frames, in addition to the data frames that were originally covered by 802.11i. The 802.11w protocol applies only to a set of robust management frames that are protected by the MFP service. These include Disassociation, De-authentication, and Robust Action frames. Unless the packets were sent by clients, the access point (AP) will not receive those packets. The purpose is to avoid DoS attacks in the network; for example, when a DoS attacker launches a Spoofed Disconnect De-authentication/Disassociation attack on an existing connection.

Note: MFP is required on both the AP and client in order to support 802.11w.

How Does It Work?

802.11w prevents Spoofed Disconnect DoS attacks

- As wireless network connection protocols develop and progress, secure encryption and authentication requirements for data transmission are also gradually increasing; therefore, in 2004, the IEEE completed the formulation of IEEE 802.11i protocol. Though IEEE 802.11i can protect data packets, it cannot protect management packets. Aware of this problem, IEEE 802.11w was ratified in 2009. IEEE 802.11w, a wireless encryption standard, was developed based on IEEE 802.11i, which prevents management packets from being attacked in wireless Local Area Networks (LANs). With the added assurance in wireless network security and reliability, VoIP applications can further rely on wireless networks to provide adequate call quality and coverage.

- IEEE 802.11w offers three main types of protection. The first is for unicast management frames, which are packets transmitted between one AP and one client. By extending the existing notion of data encryption algorithms, e.g., Temporal Key Integrity Protocol (TKIP) and RC4 encryption algorithms, IEEE 802.11w offers protection against forgeries and enables wireless communication confidentiality. The second type of protection is for broadcast management frames, wherein radio frequency properties or start measurements are adjusted instead of reporting sensitive information. In essence, there is no need to encrypt broadcast management frames, plus the encryption for broadcast packets generally is more complex than for unicast packets. IEEE 802.11w mainly protects against forgeries, such as counterfeiting and eavesdropping, rather than providing confidentiality. To achieve this, it only relies on one set of information integrity code, which is appended to the non-encrypted management packets. The last type of protection is for de-authentication and dissociation frames. With a pair of one-time keys between one AP and one client, the client can determine if the de-authentication is valid or not.

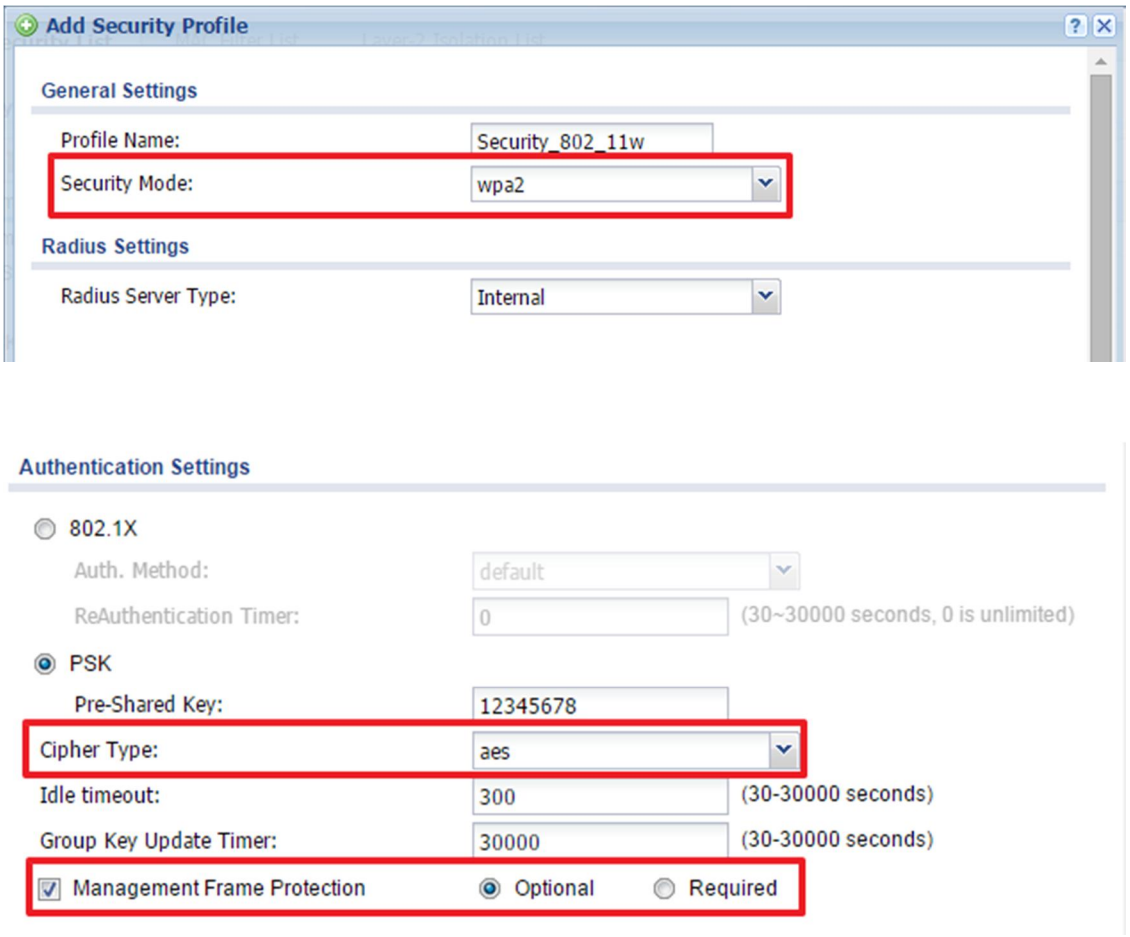
- With 802.11w implemented in the wireless network, WLAN management frames, such as de-authentication and dissociation frames between APs and client stations (STAs), are secured with the addition of cryptographic protection, wherein DoS attacks using spoofed packets are prevented.

Configuration

- Only the WPA2-AES (WPA2 with AES) security protocol is compatible with 802.11w
- Management Frame Protection: MFP (802.11w) support or not
  - Optional: If the client supports MFP, the management frames will be encrypted
  - Required: The client MUST support MFP; otherwise the authentication cannot be performed by the AP

Setting Path:

CONFIGURATION > Object > AP Profile > SSID > Security List > Authentication Settings > Management Frame Protection



Note: Default is disabled.

Application Limits

Enabling 802.11w on an AP MAY affect a client's performance. Whether it's a ZyXEL AP or another brand's AP, the same issue will be encountered. This issue should be resolved soon by chip vendors due to increasing client support for 802.11ac.

Scenario

Protecting a wireless network to avoid security threats

A wireless network hacker usually uses a tool to broadcast de-authentication and disassociation, in order to interrupt the connection between clients and the AP.

The WAC6500 series AP and its client devices must support 802.11w to avoid these kinds of wireless security threats.