Các khái niệm cơ bản về WiFi

Station vả Access Point

Thiết bị kết nối vào mạng WIFI được gọi là station (trạm). Việc kết nối vào mạng Wifi được hỗ trợ bởi một access point (AP), một AP có chức năng như một hub nhưng dùng cho nhiều station. Một access point thông thường được kết nối vào một mạng dây để phát WIFI (tức là chuyển từ mạng dây sang WIFI). Do đó access point luôn được tích hợp vào router. Mỗi access point được nhận biết bằng một SSID (Service Set IDentifier), SSID cũng là tên của mạng hiển thị khi ta kết nối vào WIFI.

Hotspot

Một hotspot là một nơi mà các thiết bị có thể kết nối Internet, và thường là bằng WiFi, thông qua mạng WLAN (wireless local area network: mạng nội bộ không dây) nối với router.

Các chuẩn bảo mật WiFi

WEP

WEP (Wired Equivalent Privacy) là một giai thuật bảo mật cho mạng không dây chuẩn IEEE 802.11. Ban đầu, các nhà sản xuất chỉ sản xuất các thiết bị WiFI với chuẩn bảo mật 64 bit. Sau này có các cải tiến hơn với các chuẩn bảo mật 128 bit và 256 bit. Bảo mật WEP sau đó xuất hiện nhiều lổ hổng. Các khóa WEP ngày nay có thể bị crack trong một vài phút các bằng phần mềm hoàn toàn miễn phí trên mạng. Vào năm 2004, với sự phát triển của các chuẩn bảo mật mới như WPA, WPÀ2, IEEE tuyên bố các chuẩn WEP trong bảo mật WiFi sẽ không còn được hỗ trợ.

WPA

WPA (Wi-Fi Protected Access) là giao thức và chuẩn bảo mật WiFi phát triển bởi Liên hiệp Wifi (Wifi Alliance). WPA được phát triển để thay thế cho chuẩn WEP trước đó có nhiều lỗ hổng bảo mật.

Phiên bản phổ biến nhất của WPA là WPA-PSK (Pre-Shared Key). Các kí tự được sử dụng bởi WPA là loại 256 bit, nên tính bảo mật sẽ cao hơn rất nhiều so với mã hóa 64 bit và 128 bit có trong hệ thống WEP. Trong WPA có hỗ trợ TKIP (Temporal Key Integrity Protocol). TKIP sử dụng các gỉai thuật để đảm bảo an toàn cho các gói tin truyền trong WIFI để tránh bị đánh cắp. Tuy nhiên TKIP sau này cũng bộc lộ một số lổ hổng bảo mật và bị thay thế bởi AES (Advanced Encryption Standard). Giao thức AES được dùng trong cả WPA và WPA 2.

WPA 2

WPA 2 (WiFi Protected Access II) là giao thức và chuẩn bảo mật thay thế cho WPA từ năm 2006 và được xem là chuẩn bảo mật an toàn nhất đến thời điểm này. Ngoài việc sử dụng giao thức AES,thì WPA 2 còn sử dụng thêm giao thức mã hóa CCMP (CTR mode with CBC-MAC Protocol). Giao thức CCMP là một giao thức truyền dữ liệu và kiểm soát tính truyền dữ liệu thống nhất để bảo đảm cả tính bảo mật và nguyên vẹn của dữ liệu được truyền đi. Cho đến nay thì giao thức bảo mật WPA2 dùng AES là giao thức bảo mật Wifi tốt nhất.