Cisco Networking Academy® Mind Wide Open™

Configuring Wireless Access Point

Subhrendu Guha Neogi **(4 mins)**

Whenever we configure any wireless access point, first we need to connect this particular access point to a PC via wired network for configuration purpose.

While configuring wireless port, first, the best practice is we should not use the default SSID that comes from the factory or from the manufacturer. We need to configure the SSID, a proper SSID. SSID is the Service Set Identifier, this identifies this access point in the network.

If we have multiple wireless access points and a single access point controller, we should have all the access points with the same kind of configuration for better connectivity. Same kind of configuration means same SSID, same type of authentication or passwords. If we talk about best practice, we need to create a meaningful SSID for the network.

When configuring the authentication; we check different authentication mode. The first one is called WEP, and second one is called WPA – WiFi Protected Access. We have WPA and WPA2. These are the three different types of security modes available that we can configure authentication - WEP, WPA and WPA2.

First, we need to check what is available with the client and this is very much required when we are configuring authentication. We need to choose authentication and the encryption type. When we are talking about WEP, this also have a security algorithm, which is a traditional standard that came with IEEE 802.1. We still do not use WEP now.

The second one, which we use is basically WPA and WPA2. The difference between WPA and WPA2, is WPA uses TKIP, and WPA2 is using AES. TKIP - Temporal Key Integrity Protocol; if we are choosing encryption type TKIP, this is no longer secure. The best practice is we should useWPA2 - the best one, which use Advanced Encryption Standard (AES) algorithm. In WPA2, we have two types of methods. One is WPA Standard (Personal), and one is Advanced (Enterprise).

In Enterprise, there is something called PSK, which is called Pre-Shared Key. This require a RADIUS server. If we have a large enterprise or a bigger WiFi network, we need to provide username and password for each and every user. Hence we need to use the RADIUS server to manage this information to provide a advanced level of authentication by giving each and every user a particular user name and password.

The next one is called MAC Authentication, which is a best practice. We should also disable SSID Broadcast and also go for MAC Authentication. MAC Authentication can restrict end devices, such as, you want to block any particular PC or laptop we can do so. The best practice is to store every device’s MAC address is stored in the access point or access point controller.