Wireless Router Wireless and Security Settings

Subhrendu Guha Neogi (**6.5 mins**)

We come to the most important part, where we need to configure our wireless devices. In the Wireless tab, we have the basic configuration. If we have WiFi Protected Setup, we can always use the wizard mode for configuration.

We can also do manual configuration. In manual configuration, we need to set the wireless band. I am using 2.4 GHz. Next, you can choose the radio mode: BG-Mixed, Wireless-G, B, N or mixed mode. I am choosing mixed mode.

Next is choosing SSID. This is required so that your wireless device can be identified in the network. Once you choose your SSID, then this needs to be provided to all wireless clients - those want to be connected with you.

Next is Channel Width, and numbers of channel, and types of channels. You can choose 'Auto' input in both cases.

It is a best practice to disable ‘SSID Broadcast’. If you enable it, any client can see your SSID. It is better that you manually set SSID in your end-user devices and clients.

Thus for Wireless Security - two best practices we have: one is choosing SSID, next is disabling SSID broadcast.

In basic configuration we have Wireless Network Name, Channel, and types of channels, and finally the SSID Broadcast- enable or disable.

Next is Wireless Security Mode. So these are the different security modes available. The old security mode is WEP(Wired Equivalent Privacy) which comes with IEEE802.11 standard. This was revised and it is sometimes call IEEE 802.11i standard, which was available in the year 2003.

Once you select WEP, it will give you a warning and after that you can choose your encryption standard. Let's choose a higher weight encryption standard, and giving a password ‘CISCO', and then you can generate a key. You can see the key is generated. This is not secure, so we need to avoid WEP.

The next standard is called the WPA (WiFi Protected Access). There are two options: WPA Personal and WPA Enterprise.

Once you choose WPA Personal encryption standard, you have to provide the password, which is called 'passphrase'. This will use the encryption standard, which is called TKIP- Temporal

Key Integrity protocol. This is a stopgap encryption protocol, which was introduced after replacing WEP encryption.

Both methods are similar; the functionality of TKIP and WEP. The security feature is not so good, but the security functionality is (the) same. That is the reason we do not use TKIP. It may happen that your client does not support WPA2, then you have to use TKIP.

The best is to use WPA2. When you use WPA2 Personal, you can always configure a mixed mode so that both types of clients can be connected.

When you select WPA2, it is using Advanced Encryption Standard (AES) encryption. This is more secured and came after 2005. It is found that AES encryption is better, and more secure. We can use a strong passphrase, which can prevent a brute force attack.

Where appropriate, we should use WPA2 Enterprise. Whenever we use WPA2 Enterprise, we need to use a RADIUS server. This RADIUS server will provide authentication, and there is a pre-shared key, which is called PSK. This PSK is generally the encryption passphrase, which is required to be shared with the RADIUS server.

You can change the port - this is better wireless security, because the attacker cannot understand which port they are exchanging the password, so it is not easy to hack.

We will be using a unique key. This unique key is shared amongst the RADIUS server and your wireless devices.

WPA2 uses AES for basic authentication, and after that, the RADIUS server will provide the username and password. As far as security is concerned, this is better.

The next part is Wireless MAC Address Configuration. The best practice is that we need to enable Wireless MAC Filter.

There are two options. All the devices in this topology are connected to this wireless access point. If I want to block some, I can still do it by providing the devices' MAC addresses. If I want to block a particular device we can do the same.

This is the best secure mechanism where we can have only the devices registered with this wireless router to get access. Once you provide the proper MAC addresses, then only these devices can be connected to the network.

The next part is Advanced Wireless Settings where we can check the Basic Rate, Antenna Selections, and all those advanced features, which are pertaining to the connectivity.

Next is 'Security'. It is always better to enable the Firewall Protection. We can also use a third-party firewall or the Internet filter in that device such as Multicasting, NAT Redirection, some Proxy Server Settings.