Instructions for changing settings in Wi-Fi Router

Whether you have a wireless router or multiple access points (APs), there are a number of settings and features that you can use to improve your Wi-Fi network. And many of them help increase performance and security.

TipsMake.com - Whether you have a wireless router or access point (AP), there are a number of settings and features that you can use to improve your Wi-Fi network. And many of them help increase performance and security. So go to the router's Web-based configuration page or AP to see which settings will help us improve network performance.

Wireless Security (Wireless Security)

There are three main security options for Wi-Fi for secure encryption and password protection: WEP, WPA and WPA2. Never use WEP because it can be cracked easily. Please use WPA2 to get the best protection. And if any old Wi-Fi device or adapter does not support WPA2, replace them with a newer version.

Also keep in mind that both the WPA and WPA2 security versions can be used in two very different modes: personal mode (PSK) and business mode (802.1X authentication).

Personal mode settings are extremely simple. Just create a password on the router or AP and then import it to your computer and Wi-Fi device when you want to connect. However, this mode is not suitable for businesses

because they do not want to change passwords every time employees leave. Users will have to change the password for the entire wireless router and re-enter the new password for each device and device on the Wi-Fi network.

However, the mode for businesses is more secure because we can create a login name and password for each user who then grants or regains access anytime. This mode requires installing a RADIUS server.

Wireless Channel (Wireless Channel)

There are 11 channels (in the US) that Wi-Fi devices can use. However, note that channels may overlap between different Wi-Fi networks. Therefore, when we install the channel, it should be noted that channels on routers or access points with overlapping coverage cannot be the same. Otherwise they will interfere with each other. Therefore, before installing the channel, check which channels are used by neighboring wireless networks.

Wireless mode (Wireless Mode)

802.11n and 802.11ac wireless transmission standards all support backward compatibility. By default, most wireless routers and access points support all older standards. However, when there are multiple wireless devices that use the old standard that connect to the 802.11n router, the router can reduce speed and performance. So if all computers support 802.11n, change the wireless mode to 802.11n.

Channel Width (Channel Width)

To get real speed from 802.11n or 802.11ac standards, you have to change the router's wireless channel width. The 802.11b and 802.11g standards only use 20MHz wide channels, but 802.11n supports up to 40MHz to achieve higher transmission speed. So, if your Wi-Fi device supports 802.11n, change the channel width to 40MHz.

Promote SSID (SSID Broadcasting)

Wireless routers and APs default to the network name (SSID) so other devices can detect the signal. But we can disable this feature, hide the network. And when you want to connect to the hidden network, users must manually enter the network name so that the computer knows the connected SSID. This is also considered an additional security but this can have a negative impact on network performance and not an effective solution against hackers.

Guest Network (Guest Network)

Some routers have a feature that enables the activation of a second Wi-Fi signal with the SSID network name and privacy settings. This is a way of providing quick access and security for visitors, or being able to create a separate network for some groups of users such as managers so they are not on the same network as regular employees. . Just make sure you enable the split option or block access to the main private network. And to prevent anyone nearby from connecting to the wireless Internet, we should also set up WPA2 security for this guest network.

Quality of Service (QoS)

Most routers and APs have a number of QoS quality levels that allow users to prioritize radio traffic based on traffic type. For example, prioritize traffic for online applications such as video conferencing over regular network traffic such as web browsing and file downloading.

Create multiple VLANs and SSIDs

Many enterprise class routers support virtual LAN (VLAN) features and multiple SSIDs so we can create and use multiple virtual networks separately. For example, you want the management department to be on the same VLAN / SSID to share sensitive data, other VLANs / SSIDs for employees so that they cannot access VLAN / SSID management side or VLAN / SSID anymore for guests Internet access only.

Usually each VLAN comes with a unique ID. Use VLAN ID assigned to Ethernet ports on the switch. Or if using 802.1X authentication, we can assign each user a VLAN ID and when they connect to the network, it automatically assigns a VLAN ID regardless of where they connect.

summary

Remember, disabling SSID promotion doesn't really mean much security while reducing performance and complicating connection processing. But, you can invest in a RADIUS server or hire a server service to be able to use the enterprise mode (802.1X authentication) of WPA2. And if the router has a guest network feature or VLAN support, you can create multiple ways to access Wi-Fi for different types of users and guests.

To reduce noise in Wi-Fi networks, make sure that the radio channels are not the same between adjacent networks. Depending on the Wi-Fi standard in use, change the default wireless mode and the channel width to be reasonable. And make sure high-bandwidth devices get enough bandwidth through QoS according to the traffic.