Compare 4 types of security WiFi WEP, WPA, WPA2 and WPA3

Wireless security is extremely important. The vast majority of us connect a mobile device, such as a smartphone, tablet, laptop, or other device, with a router at many times of the day.

Wireless security is extremely important. The vast majority of us connect a mobile device, such as a smartphone, tablet, laptop, or other device, with a router at many times of the day. Moreover, Internet of Things devices also connect to the Internet with WiFi.

They are always active, always 'listening' and always need high security. Therefore, WiFi coding steps are extremely necessary. There are several different ways to protect WiFi connection. But how do users know which WiFi security standard is best? The following article will help you answer this question.

WEP, WPA, WPA2 and WPA3 - What is the best security type?

Types of WiFi security

The most popular types of WiFi security are WEP, WPA and WPA2.

Compare WEP and WPA

Wired Equivalent Privacy (WEP) is the oldest and least secure WiFi encryption method. The way WEP protects WiFi connections is so bad, so if you're using WEP, you need to change this type of security immediately.

1. Upgrade WiFi security from WEP to WPA2

Moreover, if you are using an old router that only supports WEP, users should upgrade it for better security and connectivity.

Why? Cracks (crackers who are good at computers, but only illegally using their talents to serve their own interests) have found a way to break WEP encryption and this is done easily. with tools available for free. In 2005, the FBI made public arguments about using free tools to raise people's awareness. Almost everyone can do it. Therefore, the WiFi Alliance officially abandoned the WEP standard in 2004.

At the present time, users should use WPA version.

Definitions of WPA and WPA2

The non-secure WEP standard was formerly a precursor to WiFi Protected Access (WPA). WPA is just a buffer for WPA2.

When WEP became insecure, the WiFi Alliance developed WPA to provide network connections with an additional layer of security before developing and introducing WPA2. WPA2 security standards are always desirable goals.

WPA3

Currently, most routers and WiFi connections use WPA2, because it is still safe from many vulnerabilities in encryption standards.

However, the latest upgrade for WiFi Protected Access - WPA3 has appeared. WPA3 possesses some important improvements to modern wireless security, including:

1. **Protection from Brute Force** : WPA3 attacks will protect users, even if they use weak passwords, from Brute Force attacks.
2. **Public network security** : Additional WPA3 encrypts personal data, theoretically, encrypting a user's connection to a wireless access point, regardless of the password.
3. **Internet of Things security** : WPA3 came at a time when Internet of Things device developers were under enormous pressure to improve facility security.
4. **Stronger encryption** : WPA3 adds 192-bit stronger encryption, significantly improving security levels.

WPA3 has not yet entered the consumer router market, although as expected, this should have happened by the end of 2018. The transition from WEP to WPA and from WPA to WPA2 took a long time, so There is nothing to worry about at the moment.

Moreover, manufacturers have to release devices that are backwards compatible with bug fixes, which can take months, even years.

Compare WPA, WPA2 and WPA3

The phrase WiFi Protected Access is repeated up to 3 times. WPA and WPA2 are already too familiar, but WPA3 seems a bit strange, but it will soon appear on the router. So what are the different types of security? And why is WPA3 better than WPA2?

WPA is vulnerable to attack

WPA is almost 'no door' when putting on the balance table with the other two competitors. Although it has a strong public key encryption feature and uses WPA-PSK 256-bit (Pre-Shared Key), WPA still has some 'inherited' vulnerabilities from the old WEP standard (both have the same Vulnerable stream encryption standard, RC4).

The vulnerability focuses on the introduction of the Temporal Key Integrity Protocol (TKIP).

TKIP itself is a big step, because it uses a key system on each package to protect each packet sent between devices. Unfortunately, deploying TKIP WPA must take into account older WEP devices.

The new TKIP WPA system has 'recycled' some aspects of the vulnerable WEP system and, of course, the same vulnerabilities have also appeared in the new standard.

WPA2 replaces WPA

WPA2 officially replaced WPA in 2006. But anyway, WPA once had a short time as the 'pinnacle' of WiFi encryption.

WPA2 offers another security and encryption upgrade, most notably the introduction of Advanced Encryption Standard (AES) for consumer WiFi networks. AES is significantly stronger than RC4 (because RC4 has been 'cracked' many times) and is the security standard applied to many online services at the present time.

WPA2 also introduced Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (Blocked Authentication Code Protocol), called CCMP for short, to replace TKIP now vulnerable.

TKIP is still part of the WPA2 standard, as well as providing functionality for WPA-only devices.

KRACK WPA2 attack

KRACK attack is the first vulnerability found in WPA2. The Reinstallation Attack (KRACK) key is a direct attack on the WPA2 protocol and unfortunately weakens any WPA2 WiFi connection.

Basically, KRACK weakens the important aspect of WPA2's 4-step handshake process, allowing hackers to block and manipulate the creation of a new encryption key in a secure connection process.

But even if KRACK is so powerful, it is very likely that someone will use this tool to attack the home network.

1. Instructions on how to protect WiFi network from KRACK

WPA3: Response of WiFi Alliance

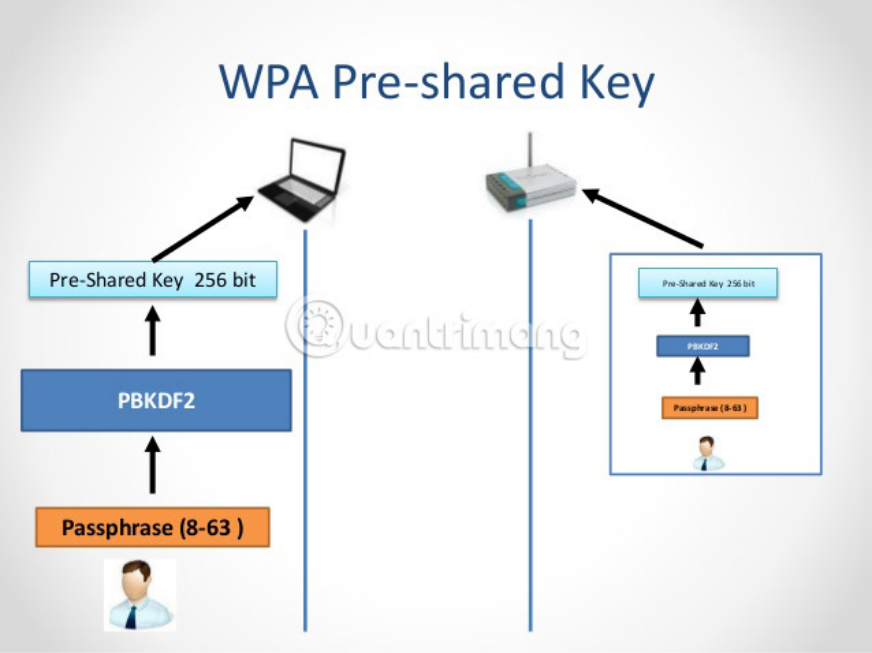
WPA3 was born a bit late but provided much higher security. For example, WPA3-Personal provides encryption for users even when hackers have 'unlocked' the password after connecting to the network.

Furthermore, WPA3 requires all connections to use Protected Management Frames (PMF). PMF basically enhances privacy protection, with additional security mechanisms for data security.

A 128-bit AES standard remains the same for WPA3 (a testament to its 'permanent' security). However, WPA3-Enterprise connections still need AES 198-bit. WPA3-Personal users will also have the option to use high-intensity AES 198-bit.

To discover more new features of WPA3, please refer to the article: Learn about WPA3, the latest WiFi security standard today.

What is WPA2 Pre-Shared Key?



WPA2-PSK stands for Pre-Shared Key, also known as Personal mode, exclusively for small office networks and home networks.

Wireless router encrypts network traffic with a key. With WPA-Personal, this key is a WiFi passphrase set up on the router. Before a device can connect to the network and "understand" the encryption, the user must enter the passphrase on it.

The real weakness of WPA2-Personal encryption is a weak passphrase. Since many people often use weak passwords for online accounts, it is not uncommon for them to use the same weak passphrase to secure wireless networks. The principle is that using a strong password to secure the network or not WPA2 can not help much.

What is WPA3 SAE?

When using WPA3, users will use the new key exchange protocol called Simultaneous Authentication of Equals (SAE). SAE, also known as the Dragonfly Key Exchange Protocol, is a more secure key exchange method to address the KRACK vulnerability.

Specifically, it is able to resist offline decryption attacks by providing Forward secrecy (which is part of the communication process between the browser and the server via HTTPS protocol). Forward secrecy prevents an attacker from decrypting a previously recorded internet connection, even if they know the WPA3 password.

Also, WPA3 SAE uses peer-to-peer connectivity to establish communication and eliminate the possibility of a malicious intermediary blocking the keys.

What is WiFi Easy Connect?

WiFi Easy Connect is a new connection standard designed to simplify the provision and configuration of WiFi devices.

In it, WiFi Easy Connect provides strong public key encryption for each device added to the network, even applications with little or no user interface, such as smart houses and IoT products. .

For example, in the home network, the user will assign a device as a central configuration point. The central configuration point must be a multimedia device, such as a smartphone or tablet.

After that, the multimedia device is used to scan the QR code, in turn running the designed WiFi Easy Connect protocol of the WiFi Alliance.

Scanning a QR code (or entering a specific code for an IoT device) gives the device the same security and encryption as other devices on the network, even if direct configuration is not possible. WiFi Easy Connect, in conjunction with WPA3, will enhance the security of IoT networks and smart home devices.

WiFi security is extremely important

At the time of writing, WPA2 is still the most secure WiFi encryption method, because it counts even the KRACK vulnerability. Although KRACK is definitely a problem, especially for corporate networks, it is unlikely that ordinary users will encounter this type of attack (unless, of course, you are a great character).

WEP is easy to crack, so it should not be used for any purpose. Furthermore, if there are devices that can only use WEP security, users should consider replacing them to enhance network security.

1. Summary of the best Wi-Fi Router devices

It should also be noted that WPA3 will not magically appear and secure all devices at a glance. Introducing a new WiFi encryption standard and applying it widely is a long process.

The success rate of this depends on whether network equipment manufacturers in general and router manufacturers in particular have applied WPA3 to their products.

At the present time, you should focus on protecting your network with WPA2.

Good luck!

See more:

1. Wireless security: Say NO to WEP and YES to WPA
2. 5 applications to secure WiFi Hotspot connections
3. Secure WiFi with advanced techniques