Common wireless encryption methods and differences

Wireless 余煌 2020-12-16 Published

Problem Description

null

Solution

WEP (Wired Equivalent Privacy): Wired Equivalent Privacy. WEP uses the RC4 stream encryption algorithm, and the initial vector IV is transmitted in plain text. Generally not used because the safety mechanism is too weak.

WPA (Wi-Fi Protected Access): WIFI access protection protocol. The authentication protocol uses the TKIP encryption algorithm (the core algorithm is RC4).

WPA2 (Wi-Fi Protected Access II): WPA2 (also known as RSN) enhances security on the basis of WPA. It is compatible with WPA and introduces CCMP (Counter Mode Cipher Block Chain Message Complete Code Protocol) instead of TKIP, and its core encryption algorithm is AES.

● It is not recommended to use only TKIP single encryption method. This encryption method limits the wireless negotiation rate to only **54Mbps!**

●The recommended encryption method is set to RSN+CCMP. This encryption method can negotiate up to **866.7Mbps** for 11ac dual-stream terminals! !

The encryption mechanism of TKIP determines its maximum negotiated rate value, which is not limited by performance on the device side~

Reference configuration

```
 wlan service-template test
  cipher-suite ccmp //recommend~
  security-ie rsn
```

PS: What if there are some old terminals in the network that are not compatible with ccmp+rsn? You can configure both combined encryption methods to let the terminal auto-negotiation~

```
 cipher-suite ccmp
 security-ie rsn
 cipher-suite tkip
 security-ie wpa
```