Contribution ID: **550**   Type: **Poster**

Security Mechanism for user access to Single SSID WLAN

Thursday, 7 November 2019 16:15 (15 minutes)

Wireless local area network (WLAN) technology is widely used in various enterprises and institutions. In order to facilitate the use of users, they often provide a single ssid access point, resulting in different identities of users authenticated and authorized can connect to the wireless network anytime, anywhere as needed and obtain the same accessible network resources such as bandwidth, access control (ACL) and so on. Multiple ssid can solve the problem but it will be confused to users who don't know which ssid can be connected. Although we could prevent visitors from accessing intranet resources by isolating the wireless network from the internal network, this would make it impossible for users to use the wireless network for internal office work. In this paper, we propose an access control sysytem that grouping users according to the different identities and users authenticated and authorized can access different network resources because a wireless access point dynamically maps an ssid provided by a mobile station to a BSSID based on a VLAN assignment. The deployment experiment of the solution proves that users of different identities accessing the same wireless network can set different access policies, which effectively improves the security of the wireless network and simplifies the management of the wireless network.

Consider for promotion

Yes

Primary author: WANG, Li (IHEP)

Presenter: WANG, Li (IHEP)

Session Classification: Posters

Track Classification: Track 7 –Facilities, Clouds and Containers