802.1X Authentication Configuration on AP541N Access Points

Objective

802.1x is a security feature used in wireless local area networks (WLANs) which follow IEEE 802.11 standards. 802.1x is an authentication framework used to authenticate clients and servers. The authentication algorithm inside the framework is not specific since there are many algorithms available. The user or supplicant who wants to access a service, requests the access point that work as the authenticator. The access point initially moves the user into an unauthorized state in which a client can send only Extensible Authentication Protocol (EAP) start messages. The access point requests the user for credentials. When the user responds with the credentials, the access point then forwards the credentials to an authentication server, which has an algorithm to authenticate the identity of the user. If the authentication is successful, the user is granted access. If not, a reject message is sent to the user.

This article explains how to enable 802.1x authentication and configure authentication information on AP541N so that the AP that acts as a middleman in the authentication process can access the authentication server.

Applicable Device

• AP541N Access Point

Software Version

• AP541N-K9-2.0(4)

802.1x Authentication

Step 1. Log in to the Access Point Configuration Utility and choose Setup > 802.1X Authentication. The 802.1X Authentication page opens:

Step 2. Click one of the Enabled or Disabled radio buttons in the 802.1X Supplicant field to enable or disable the administrative status of the 802.1X Supplicant.

Step 3. Enter the username in the Username field with which the AP is to communicate with the 802.1x authentication server.

Step 4. Enter the password associated with the username in the Password field. This is to
get access to the authentication server

Step 5. Click **Apply** to save the settings.