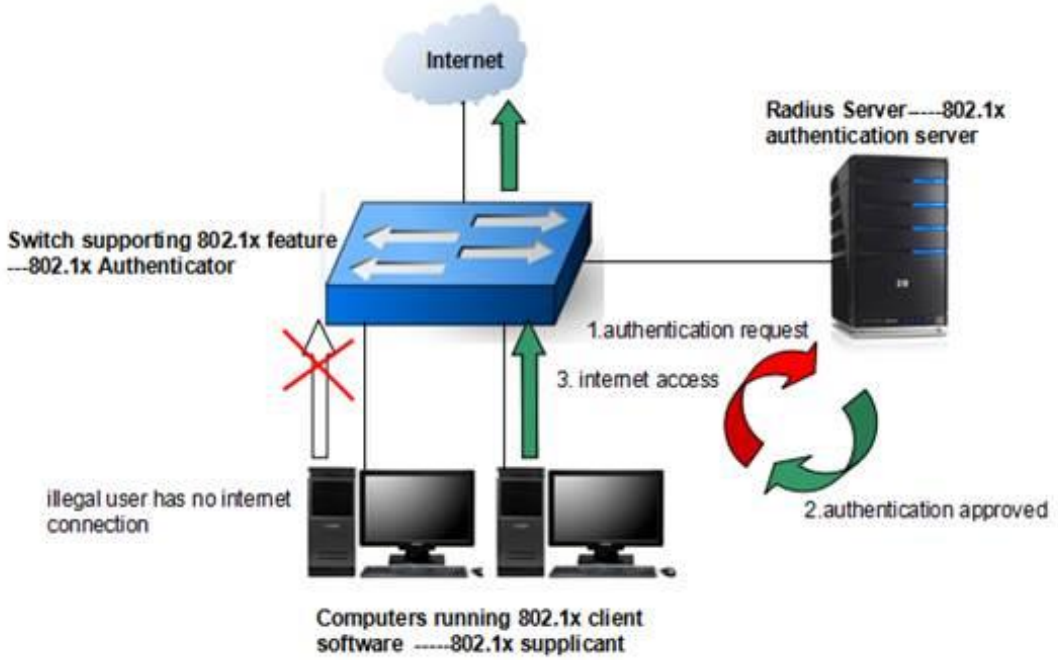
How to build up an 802.1X access authentication system using TP-LINK switch

Introduction of 802.1X Access Authentication System

802.1X access authentication system is widely used in Ethernet environment as a solution to provide authentication access for clients.

802.1X access authentication is based on "port", which means the access control and AAA authentications for clients is based on the "port" of **NAS (Network Access Server)**.If the **client** connects to the port of NAS passes the authentication of **Radius Server**, then the client can get access to the resources belonging to the NAS, but not the other way around.

Note: In this article NAS (Network Access Server) refers to TP-LINK switch which acts as 802.1X Authenticator in 802.1X system.
Computers running 802.1X client software act as 802.1X Supplicant in 802.1X system.
Computers or Servers running Radius server software act as 802.1X Authentication server in 802.1X system.
Below is the illustration of 802.1X access authentication system.

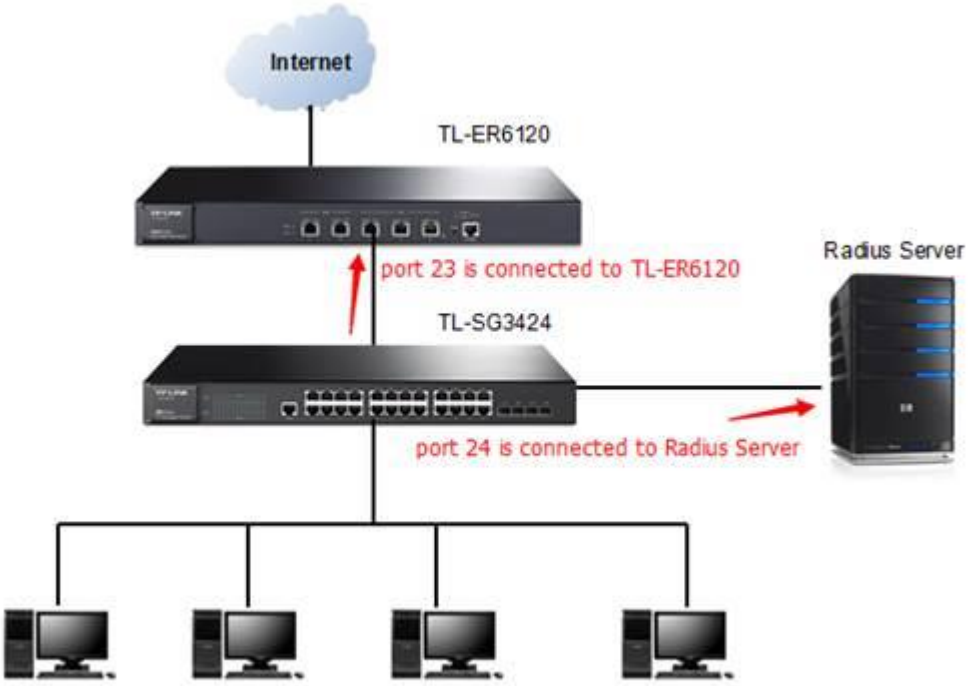


A Classic 802.1X System and Its Topology (Here we take TL-SG3424 as an example)

As is shown in the topology below, **port 24 of TL-SG3424 is connected to Radius Server** which provides the authentication, authorization and accounting for 802.1X supplicant. **Port 23 is connected to TL-ER6120** which is a router connecting to the Internet.TL-SG3424 acts as the 802.1X authenticator as well as the NAS for the system. And what we need is a system, which **only allows legal users who passed the authentication of**

Radius Server through TL-SG3424 can get internet access.

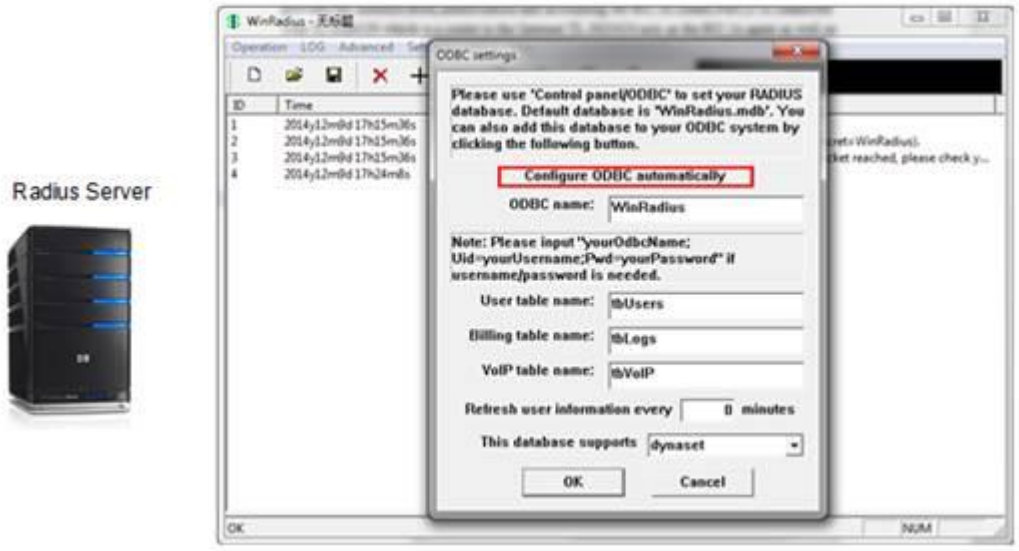
Here we will introduce the 3 steps to set up such 802.1X system.



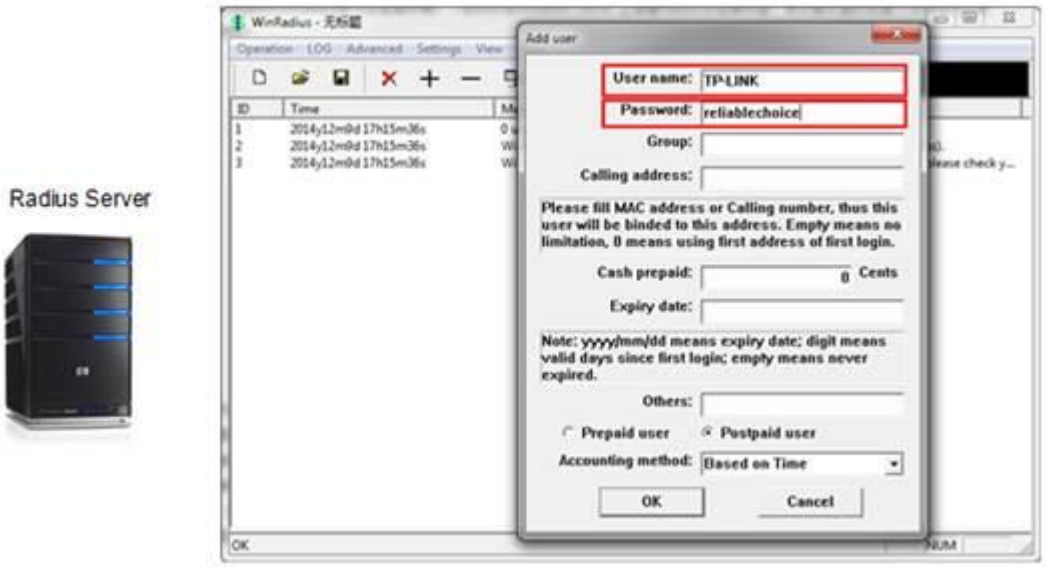
Step 1. Build up a Radius Server.

This article takes WinRadius as an example to build up a Radius Server on a local computer.(You can build up a Radius Server in Windows Server or Linux Environment as well, please refer to the related articles on how to build up Servers from the Internet)

1.1 Activate the Radius Database by click on "Configure ODBC automatically"



1.2 Add user name and password on the server.



1.3 Note down the following parameters

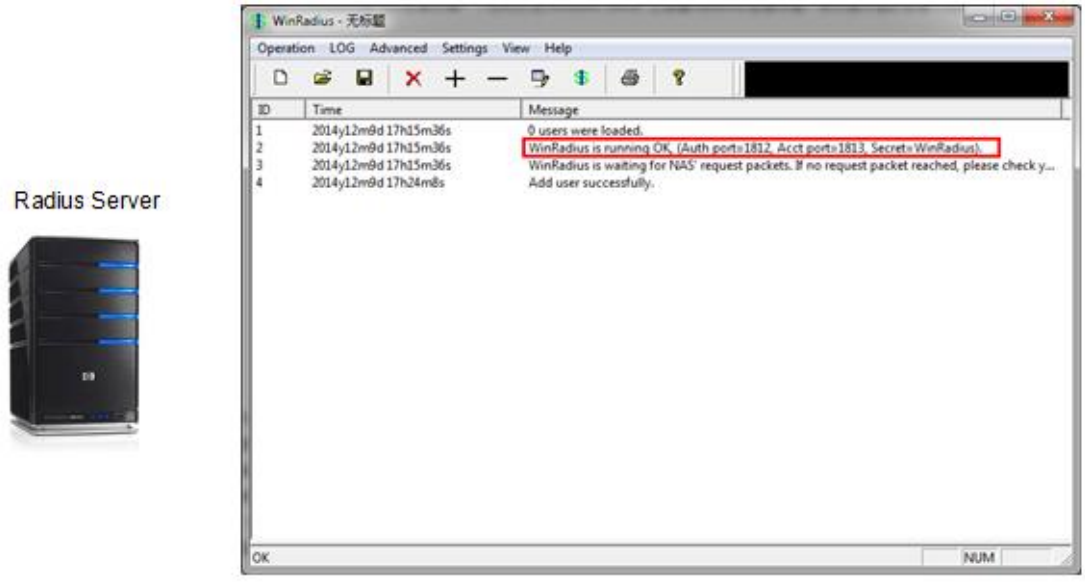
▪IP Address of Radius Server:192.168.0.100

▪Auth port=1812

▪Acct port=1813

▪Auth/Accounting Key= WinRadius

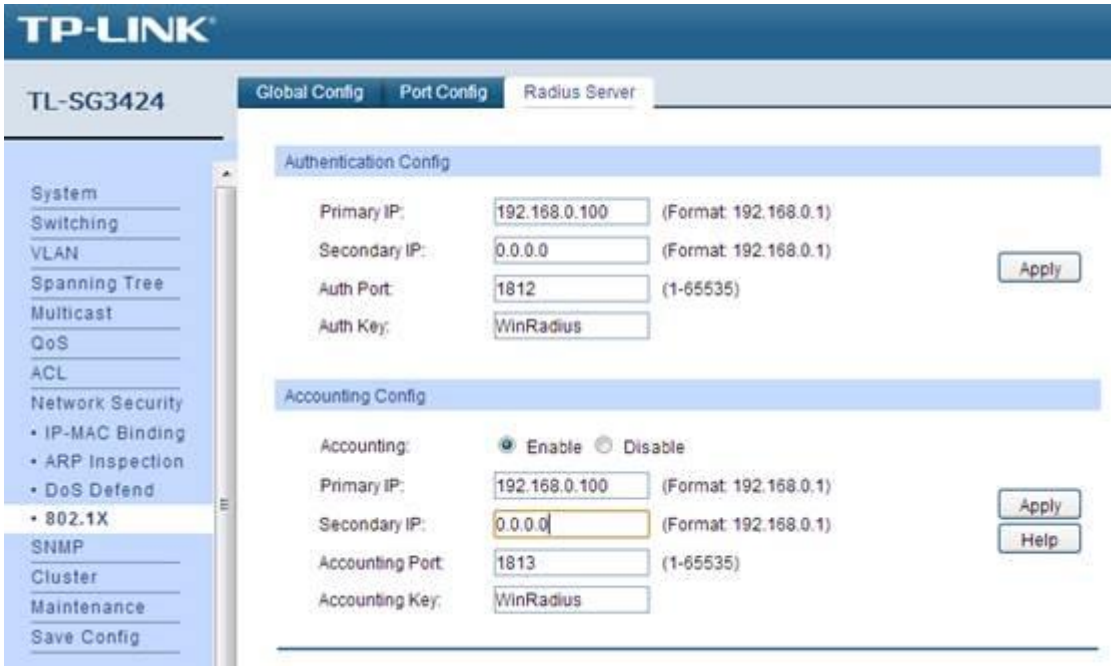
▪User name and Password



Step 2. Configure 802.1X parameters on TL-SG3424.

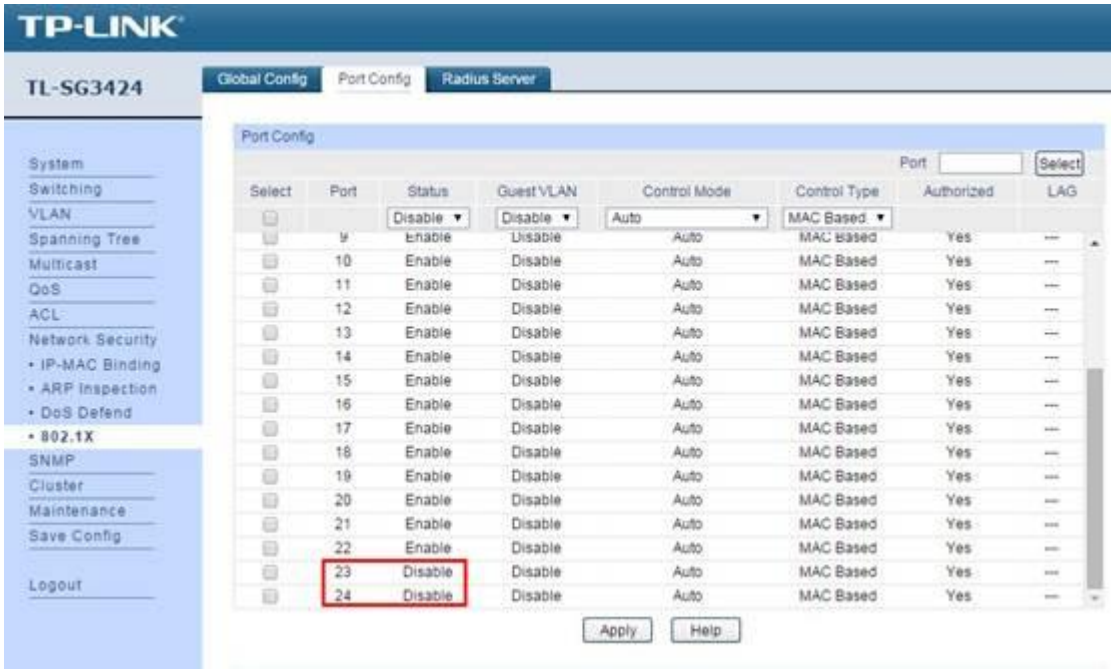
2.1 "Radius Server"

Configure the settings according to the parameters of the Radius Server (which you have noted down in **step1--"1.3"**)



2.2 "Port Config"

Disable the Status of port 23 and port 24. Enable those ports connected to 802.1X clients, which you would add to 802.1X access authentication list.



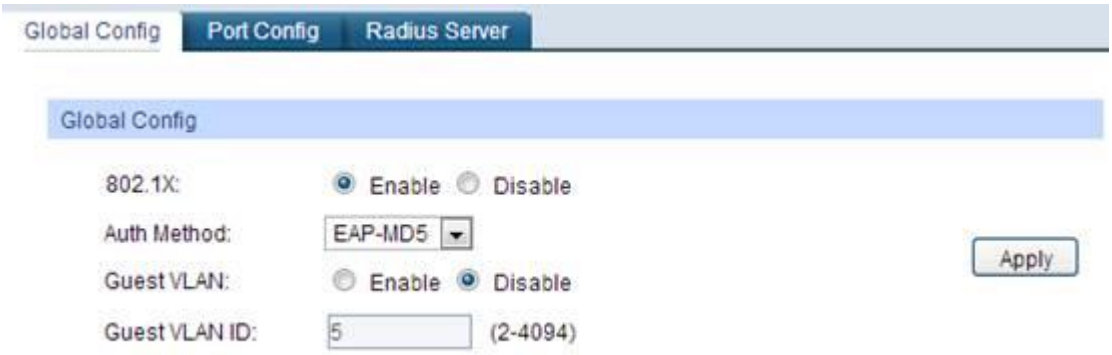
Note:

▪If "Status" of one port is **disable**, then all devices connected to this port can get access to the network **without authentication**.

▪In "Control Type", "MAC Based" indicates any device connected to the corresponding port needs independent authentication before getting access to the network. While "Port Based" indicates all devices connected to one port can get access to the network as long as one of them has passed the authentication of corresponding port.

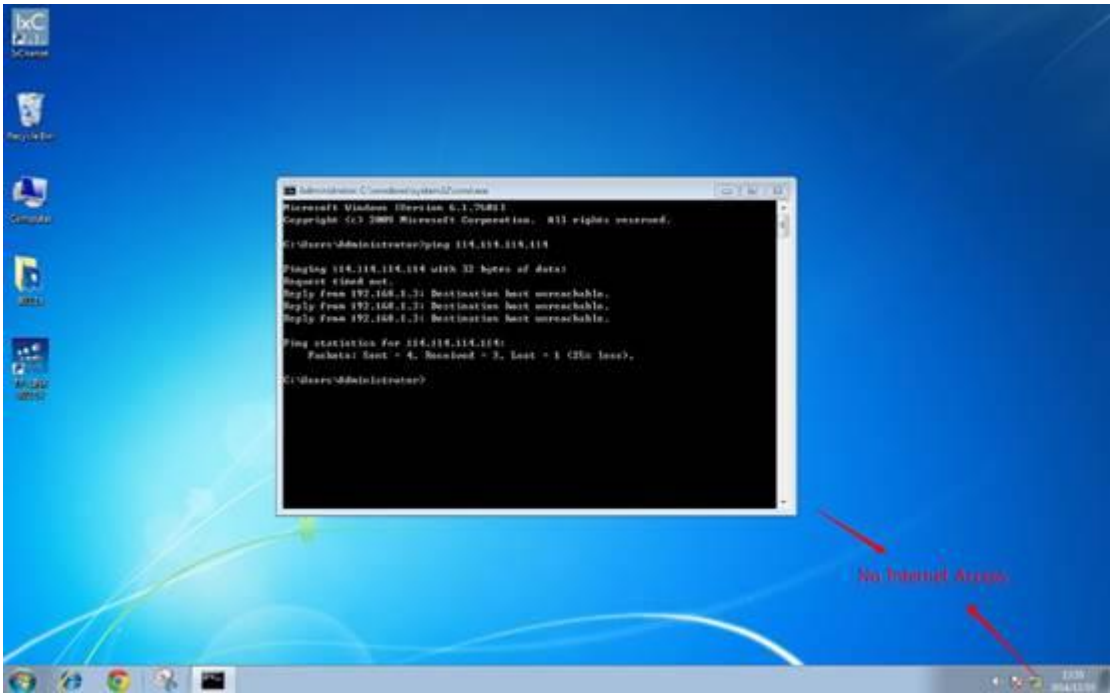
2.3 “Global Config”

Enable 802.1X on global config to accomplish the configuration on TL-SG3424.



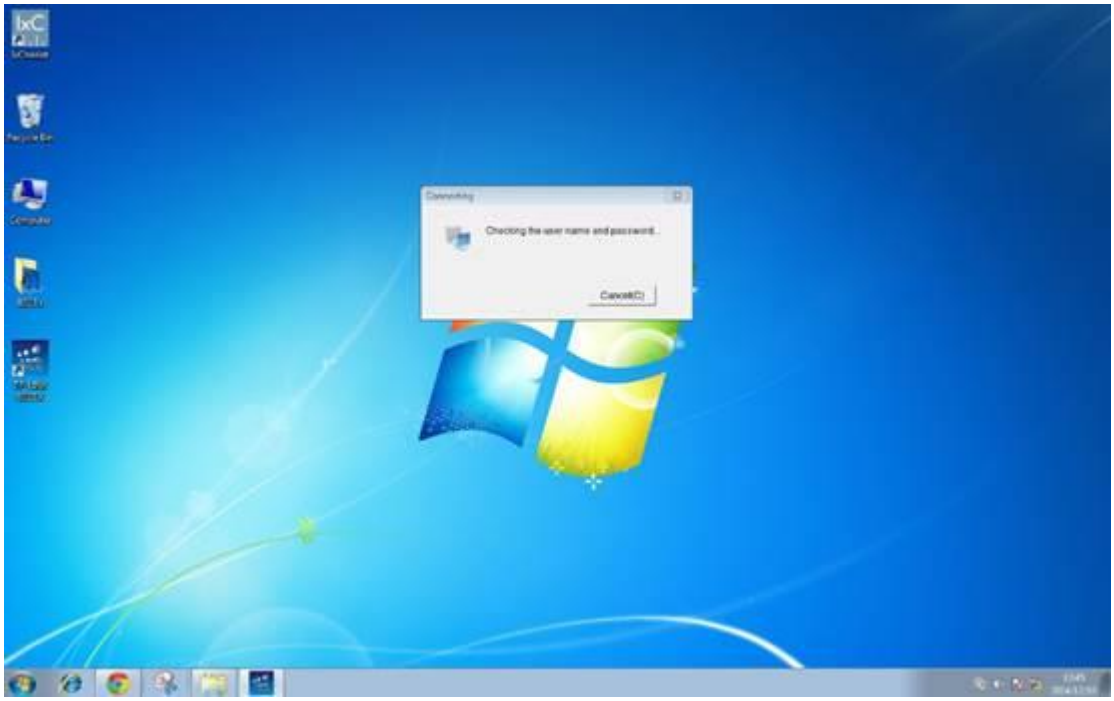
Step 3. Install TL-LINK 802.1X client software on the computers.

Before authentication, clients will not have internet access.

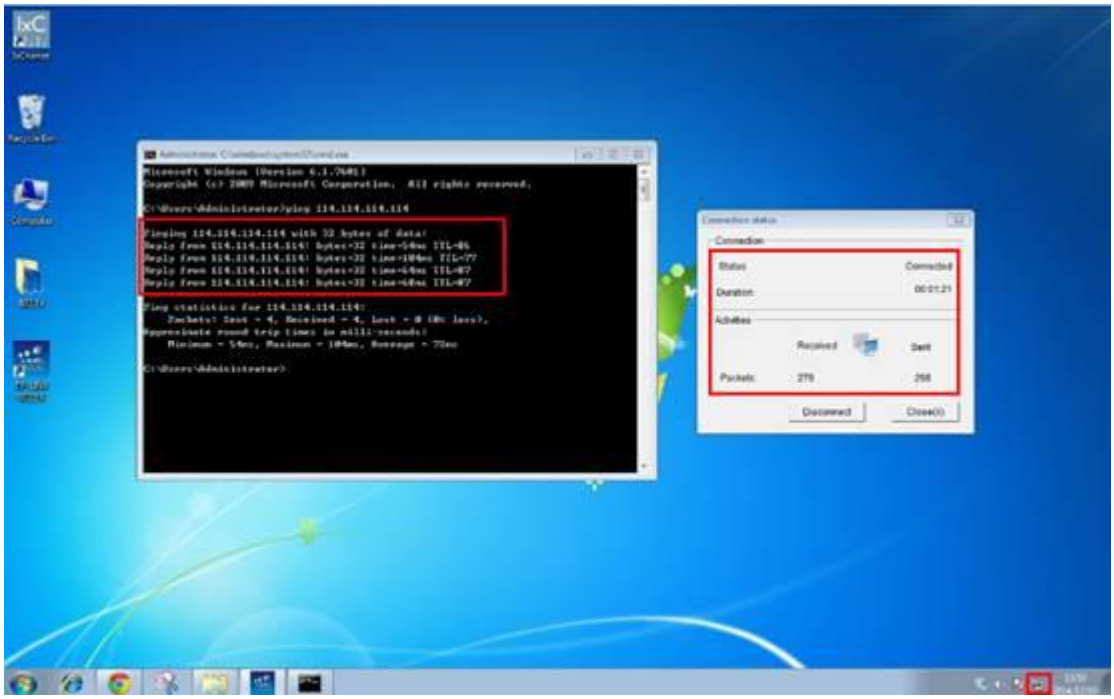


Open TP-LINK 802.1X client software, fill in the username and password, and click on “connect”.

Then the client software will automatically register to the Radius Server and get the authority to the internet from the Radius Server.



After passing authentication, the client will get access to the Internet.



Thus far, we have established a typical 802.1X access authentication system, computers in the local area network will not have Internet access unless having passed the authentication from the Radius Server through TL-SG3424.