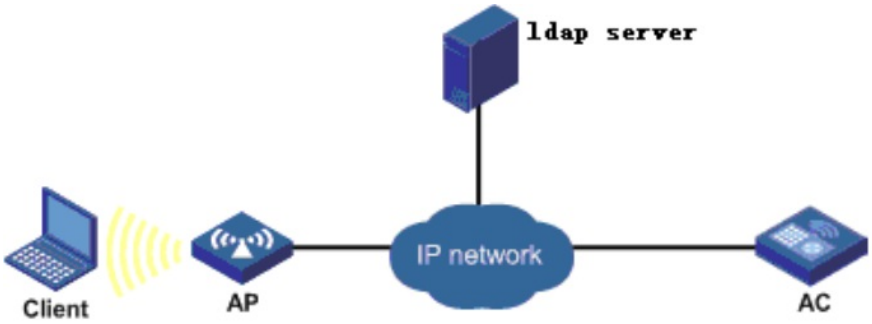
802.1x本地认证+ldap认证案例（V7）

802.1X 胡甲聪 2022-01-27 发表

组网及说明

组网如下



配置步骤

一：设备侧配置

(1) 通过ftp或者tftp方式将CA证书cacert.crt和本地证书local.pfx 导入设备。

(2) 配置pki domain，并导入证书。

#创建一个名称为eap-gtc的PKI域，导入CA证书cacert.crt和本地证书local.pfx。

[Device] pki domain eap-gtc

[Device] pki import domain eap-gtc pem ca filename cacert.crt

The trusted CA"s finger print is:

MD5 fingerprint:xxxxxx

SHA1 fingerprint:xxxxxxx

Is the finger print correct?(Y/N):y

[Device] pki import domain eap-gtc p12 local filename local.pfx

Please input the password: xxxx

(3) 配置ssl server-policy

#创建一个名称为ssl-eap 的SSL服务器端策略，配置SSL服务器策略所使用的PKI域为eap-gtc。

system-view

[Device] server-policy ssl-eap

[Device-ssl-server-policy-ssl-eap] pki-domain eap-gtc

(4) 配置eap-profile模板

#创建一个名称为eap-srv 的EAP认证方案，配置的认证方法为PEAP-GTC、引用SSL服务器端策略为ssl-eap。

[Device] eap-profile eap-srv

[Device-eap-profile-eap-srv] method peap-gtc

[Device-eap-profile-eap-srv] ssl-server-policy ssl-eap

(5) 配置全局dot1x认证

#启用EAP中继方式，支持客户端与RADIUS服务器之间所有类型的EAP认证方法。

[Device] dot1x authentication-method eap

(6) 配置ISP模板

创建一个名称为eap-gtc的ISP域，使用ldap认证、none授权和none计费方法。

[Device] domain eap-gtc

[Device-isp-local] authentication lan-access ldap-scheme ldap

[Device-isp-local] authorization lan-access none

[Device-isp-local] accounting lan-access none

[Device-isp-local] quit

(5) 配置本地ldap

创建一个名称为ldap的ldap方案，指定服务名。

[Device] ldap scheme ldap

[Device-ldap-ldap] authentication-server ldap

[Device-ldap-ldap] quit

(6) 配置ldap服务配置

创建一个名称为ldap的ldap server，指定用户名、密码、ldap服务器IP和接入方式。

[Device] ldap server ldap

[Device-server-ldap] login-dn cn=manager,dc=test,dc=com

[Device-server-ldap] search-base-dn dc=test,dc=com

[Device-server-ldap] ip 192.168.1.211

[Device-server-ldap] login-password simple xxx

[Device-server-ldap] quit

(7) 配置WLAN 服务模板

创建一个名称为10的服务模板，配置ssid、vlan、认证方式、加密套件、ISP域和eap-profile模板。

[Device] wlan service-template 10

[Device-wlan-st-10] ssid eap-gtc

[Device-wlan-st-10] vlan 300

[Device-wlan-st-10] akm mode dot1x

[Device-wlan-st-10] cipher-suite ccmp

[Device-wlan-st-10] security-ie rsn

[Device-wlan-st-10] client-security authentication-mode dot1x

[Device-wlan-st-10] dot1x domain eap-gtc

[Device-wlan-st-10] dot1x eap-termination eap-profile eap-srv

[Device-wlan-st-10] dot1x eap-termination authentication-method pap

[Device-wlan-st-10] service-template enable

二：inode配置

（1）在官网上下载最新版本的inode版本

（2）选择认证方法为peap，子类型为gtc \\ 这里的选择与AC配置中保持一致

配置关键点

（1）上述案例有版本要求，建议在5420版本之后使用

（2）本地802.1x 结合LDAP组合认证，目前设备只支持TLS和GTC这两种方式，不支持MSCHAPv2，而电脑自带客户端只支持MSCHAPv2，因此需要借助第三方工具才能实现认证，可以使用新版本的inode客户端实现 。