无线控制器AC本地802.1X认证典型配置举例(V7)

802.1X AAA 陈少华 2017-06-01 发表

Switch作为DHCP server为AP和Client分配IP地址，要求：

· 对无线用户进行802.1X认证。

· 客户端链路层认证使用开放式系统认证。

图1 本地802.1X认证组网图

注意事项

· 本地802.1X认证不支持数据加密功能。

· 本地802.1X认证不支持EAP中继认证方式。

· 目前，无线客户端只支持采用iNode智能客户端进行本地802.1X认证。

1 配置AC

(1) 配置AC的接口

创建VLAN 100以及对应的VLAN接口，并为该接口配置IP地址。AP将获取该IP地址与AC建立CAPWAP隧道。

<AC> system-view

[AC] vlan 100

[AC-vlan100] quit

[AC] interface vlan-interface 100

[AC-Vlan-interface100] ip address 2.2.2.1 24

[AC-Vlan-interface100] quit

创建VLAN 200及其对应的VLAN接口，并为该接口配置IP地址。Client将使用该VLAN接入无线网络。

[AC] vlan 200

[AC-vlan200] quit

[AC] interface vlan-interface 200

[AC-Vlan-interface200] ip address 2.2.1.1 24

[AC-Vlan-interface200] quit

(2) 配置本地用户

配置本地用户，用户名为localuser，密码为明文输入的localpass。

[AC] local-user localuser class network

[AC-luser-network-localuser] password simple localpass

配置本地用户的服务类型为lan-access。

[AC-luser-network-localuser] service-type lan-access

[AC-luser-network-localuser] quit

(3) 配置ISP域

创建名为bbb的ISP域并进入其视图。

[AC] domain bbb

为802.1X用户配置AAA认证方法为本地认证、授权和计费。

[AC-isp-bbb] authentication lan-access local

[AC-isp-bbb] authorization lan-access local

[AC-isp-bbb] accounting lan-access local

[AC-isp-bbb] quit

(4) 配置802.1X认证

配置802.1X系统的认证方法为CHAP。

[AC] dot1x authentication-method chap

(5) 配置无线服务模板

创建无线服务模板service，并进入无线服务模板视图。

[AC] wlan service-template service

配置SSID为service。

[AC-wlan-st-service] ssid service

配置无线服务模板VLAN为200。

[AC-wlan-st-service] vlan 200

配置用户接入认证模式为802.1X。

[AC-wlan-st-service] client-security authentication-mode dot1x

配置802.1X用户使用认证域为bbb。
[AC-wlan-st-service] dot1x domain bbb
使能无线服务模板。
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
创建AP，配置AP名称为office，型号名称选择WA4320i-ACN，并配置序列号210235A1GQC158004457。
[AC] wlan ap office model WA4320i-ACN
[AC-wlan-ap-office] serial-id 210235A1GQC158004457
进入Radio 1视图。
[AC-wlan-ap-office] radio 1
将无线服务模板service绑定到radio 1，并开启射频。
[AC-wlan-ap-office-radio-1] service-template service
[AC-wlan-ap-office-radio-1] radio enable
[AC-wlan-ap-office-radio-1] quit
[AC-wlan-ap-office] quit

2 配置Switch

创建VLAN 100，用于转发AC和AP间CAPWAP隧道内的流量。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
创建VLAN 200，用于转发Client无线报文。
[Switch] vlan 200
[Switch-vlan200] quit
配置Switch与AC相连的GigabitEthernet1/0/1接口的属性为Trunk，允许VLAN 100和VLAN 200通过。
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
配置Switch与AP相连的GigabitEthernet1/0/2接口属性为Access，并允许VLAN 100通过。
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
使能PoE功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
配置VLAN 100接口的IP地址。
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface100] quit
配置VLAN 200接口的IP地址。
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.1.2 255.255.255.0
[Switch-Vlan-interface200] quit
配置DHCP地址池100，用于为AP分配IP地址。
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 2.2.2.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 2.2.2.1
[Switch-dhcp-pool-100] quit
配置DHCP地址池200，用于为Client分配IP地址。
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 2.2.1.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 2.2.1.1
[Switch-dhcp-pool-200] quit

3 配置iNode智能客户端

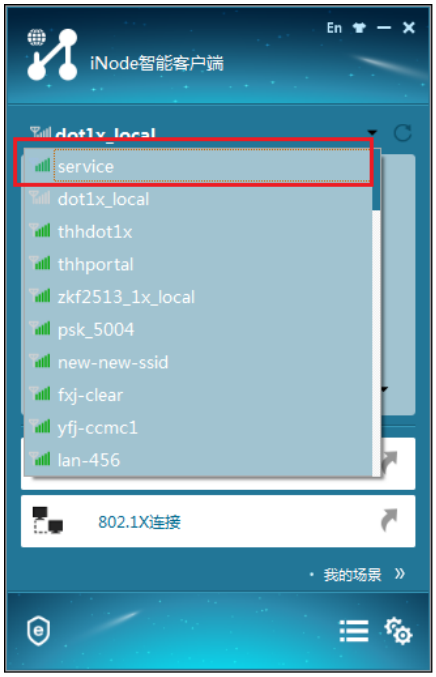
下面以iNode为例（使用iNode版本为：iNode PC 7.1），说明本地802.1x认证中iNode的基本配置。

(1)　无线连接

打开iNode智能客户端，单击“无线连接”。
图1 打开iNode智能客户端

单击无线连接右上角的小三角按钮，显示可用的无线SSID。
图1 无线连接

双击SSID为service的无线服务，进行无线网络连接。
图1 无线网络连接

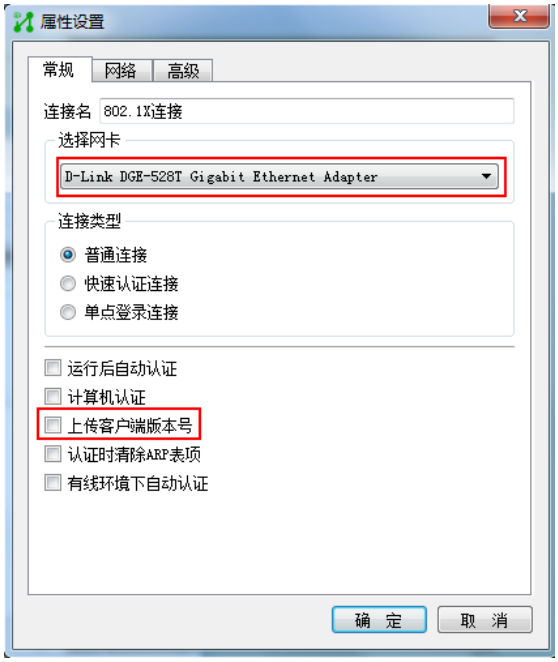


单击窗口中的<连接>按钮，接入无线网络。
图1 无线网络连接

配置802.1X认证
无线连接成功后，单击“802.1X连接”，进行802.1X认证。
图1 802.1X连接

输入用户名和密码，用户名和密码应与配置的本地认证用户名和密码相同。
图1 输入用户名和密码

单击“连接”右侧的倒三角，然后单击“属性”，进入属性设置对话框，选择当前使用的无线网卡，然后将“上传客户端版本号”前面的勾去掉，单击<确定>按钮。
图1 属性设置



最后，单击802.1X连接页面的<连接>按钮，即可进行802.1X认证。

图1 802.1X认证成功

验证配置

当无线用户通过802.1X认证成功并上线之后，AC上可以通过**display dot1x connection**命令看到上线用户的连接情况。

[AC] display dot1x connection
User MAC address : 0015-00bf-e84d
AP name : office
Radio ID : 1
SSID : service
BSSID : 741f-4ad4-1fe0
Username : localuser
Authentication domain : bbb
IPv4 address : 2.2.1.3
Authentication method : CHAP
Initial VLAN : 200
Authorization VLAN : 200
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action : N/A
Session timeout period : N/A
Online from : 2015/12/04 17:37:55
Online duration : 0h 4m 20s

AC上可以通过**display wlan service-template service**命令查看无线服务模板信息。

[AC] display wlan service-template service
Service template name : service
SSID : service
SSID-hide : Disabled
User-isolation : Disabled
Service template status : Enabled
Maximum clients per BSS : Not configured
Frame format : Dot3
Seamless roam status : Disabled
Seamless roam RSSI threshold : 50
Seamless roam RSSI gap : 20
VLAN ID : 200
AKM mode : Not configured
Security IE : Not configured
Cipher suite : Not configured
TKIP countermeasure time : 0 sec
PTK lifetime : 43200 sec

GTK rekey : Enabled
GTK rekey method : Time-based
GTK rekey time : 86400 sec
GTK rekey client-offline : Disabled
User authentication mode : 802.1X
Intrusion protection : Disabled
Intrusion protection mode : Temporary-block
Temporary block time : 180 sec
Temporary service stop time : 20 sec
Fail VLAN ID : Not configured
802.1X handshake : Disabled
802.1X handshake secure : Disabled
802.1X domain : bbb
MAC-auth domain : Not configured
Max 802.1X users : 4096
Max MAC-auth users : 4096
802.1X re-authenticate : Disabled
Authorization fail mode : Online
Accounting fail mode : Online
Authorization : Permitted
Key derivation : SHA1
PMF status : Disabled
Hotspot policy number : Not configured
Forwarding policy status : Disabled
Forwarding policy name : Not configured
FT status : Disabled
QoS trust : Port
QoS priority : 0