WX系列AC本地Portal用户访问权限控制功能的配置

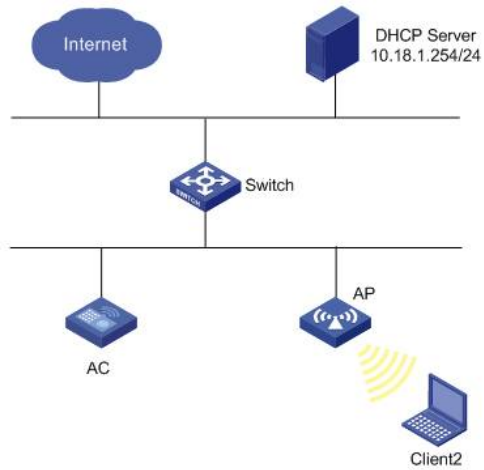
wlan接入 Portal 宋斌 2012-05-22 发表

WX系列AC本地Portal用户访问权限控制功能的配置

一、 组网需求：

WX系列AC、FIT AP、交换机、便携机（安装有无线网卡）、DHCP Server

二、 组网图：



本配置举例中的AC使用的是WX5004无线控制器（IP地址为85.3.1.220/24）。Client和AP通过DHCP服务器（IP地址为10.18.1.254/24）获取IP地址。AC与AP通过二层交换机相连，配置AC采用本地Portal方式认证来访的来宾用户。

三、 特性介绍：

基于Portal用户下发ACL的方式，实现对不同无线用户在无线接入网络中的访问权限控制，确保来宾用户只能访问特定授权的网页，保护公司内部信息的安全。

通过本设置，可以控制来宾用户的访问权限。当一个外部来宾来到公司，可以通过无线网络访问公司的一些对外资源，但是涉及公司内部的网络资源是禁止访问的。

四、 主要配置步骤：

AC配置：

配置VLAN接口及其IP地址。

```
[AC] vlan 10
[AC-vlan10] quit
[AC] interface Vlan-interface 10
[AC-Vlan-interface10] ip address 100.10.1.54 255.255.0.0
[AC-Vlan-interface10] quit
[AC] interface Vlan-interface 1
[AC-Vlan-interface1] ip address 100.1.1.54 255.255.0.0
[AC-Vlan-interface1] quit
```

配置GE1/0/1和GE1/0/2加入VLAN。

```
[AC] interface GigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1] port hybrid vlan 1 to 10 tagged
[AC-GigabitEthernet1/0/1] quit
[AC] interface GigabitEthernet 1/0/2
[AC-GigabitEthernet1/0/2] port hybrid vlan 1 to 10 tagged
[AC-GigabitEthernet1/0/2] quit
```

配置到Radius服务器的静态路由。

```
[AC] ip route-static 0.0.0.0 0 100.1.1.254
```

配置认证域

```
[AC] radius scheme acs
[AC-radius-acs] primary authentication 8.100.0.4 key cipher testkey
[AC-radius-acs] quit
```

```
[AC] domain acs
[AC-isp-acs] authentication lan-access radius-scheme acs
[AC-isp-acs] authorization lan-access none
[AC-isp-acs] accounting lan-access none
[AC-isp-acs] quit
```

开启端口安全，配置EAP认证方式。

```
[AC] port-security enable
[AC] dot1x authentication-method eap
```

配置WLAN-ESS接口。

```
[AC] interface WLAN-ESS10
[AC-WLAN-ESS10] port link-type hybrid
[AC-WLAN-ESS10] port hybrid  pvid vlan 10
[AC-WLAN-ESS10] mac-vlan enable
```

配置端口安全为802.1X方式

```
[AC-WLAN-ESS10] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS10] undo dot1x handshake
[AC-WLAN-ESS10] undo dot1x multicast-trigger
[AC-WLAN-ESS10] dot1x mandatory-domain acs
[AC-WLAN-ESS10] quit
```

在AC上配置动态WEP方式加密的无线服务

```
[AC] wlan service-template 11 crypto
[AC-wlan-st-11] ssid dweptest
[AC-wlan-st-11] bind WLAN-ESS 10
[AC-wlan-st-11] cipher-suite wep104
[AC-wlan-st-11] wep mode dynamic
[AC-wlan-st-11] service-template enable
[AC-wlan-st-11] quit
```

在AC的AP视图下配置AP名称为wa2210，型号名称这里选择WA2210-AG。请根据AP的实际型号和序列号进行配置。

```
[AC] wlan ap wa2210 model WA2210-AG
[AC-wlan-ap-wa2210] serial-id 210235A22W0079000278
```

进入AP的radio1射频视图，配置服务模板与射频1进行关联，使能AP的radio 1射频。

```
[AC-wlan-ap-wa2210] radio 1
[AC-wlan-ap-wa2210-radio-1] service-template 11 vlan-id 10
[AC-wlan-ap-wa2210-radio-1] radio enable
[AC-wlan-ap-wa2210-radio-1] quit
[AC-wlan-ap-wa2210] quit
```

配置本地portal server。

```
[AC] portal server local ip 85.3.1.220
[AC] portal local-server http
```

配置portal用户的认证域

```
[AC] domain system
[AC-isp-system] authentication portal local
[AC-isp-system] authorization portal local
```

创建VLAN接口，并启用portal，指定portal认证域。

```
[AC] interface Vlan-interface 10
[AC-Vlan-interface10] ip address 85.3.1.220
[AC-Vlan-interface10] portal server local method direct
[AC-Vlan-interface10] portal domain system
```

创建WLAN-ESS接口，并配置VLAN。

```
[AC] interface WLAN-ESS 2
[AC-WLAN-ESS2] port access vlan 10
```

配置无线服务，创建clear类型的服务模板，配置当前服务模板的SSID为portal。

```
[AC] wlan service-template 3
[AC-wlan-st-3] ssid portal
```

将WLAN-ESS接口绑定到服务模板，并使能无线模板。

```
[AC-wlan-st-3] bind WLAN-ESS 2
[AC-wlan-st-3] service-template enable
```

创建AP模板，其名称为ap22，型号名称这里选择WA2220E-AG。（注意：AP的配置需要根据具体AP的型号和序列号进行配置）

```
[AC] wlan ap ap22 model WA2220E-AG
```

设置AP的序列号为210235A29F007C000182。

```
[AC-wlan-ap-ap22] serial-id 210235A29F007C000182
```

进入radio2射频视图，将服务模板与射频关联，并使能AP射频。

```
[AC-wlan-ap-ap22] radio 2
[AC-wlan-ap-ap22-radio-2] service-template 3
[AC-wlan-ap-ap22-radio-2] radio enable
[AC-wlan-ap-ap22-radio-2] quit
[AC-wlan-ap-ap22] quit
```

配置ACL（此ACL不能包含基于源地址的规则）。

```
[AC] acl number 3322
[AC-acl-adv-3322] rule 0 permit ip destination 8.1.1.16 0
[AC-acl-adv-3322] rule 5 permit ip destination 8.1.1.20 0
[AC-acl-adv-3322] rule 10 deny ip
```

创建来宾用户，设置来宾用户密码、服务类型、过期时间、用户角色和授权ACL。

```
[AC] local-user guest
[AC-luser-guest] password simple guest
[AC-luser-guest] service-type portal
[AC-luser-guest] expiration-date 18:00:00-2011/1/31
[AC-luser-guest] authorization-attribute user-role guest
[AC-luser-guest] authorization-attribute acl 3322
```

五、 结果验证：

（1）使用命令行display portal user all查看是否有用户在线。

```
display portal user all
 Index:1919
 State:ONLINE
 SubState:NONE
 ACL:3322
 Work-mode:stand-alone
 MAC             IP              Vlan   Interface
 --------------------------------------------------------------------------------
 001e-c144-472e  85.3.1.100      10     Vlan-interface10
 Total 1 user(s) matched, 1 listed.
```

（2）通过命令行display connection ucibindex查看用户连接的详细信息。

```
dis connection ucibindex 1919
Index=1919, Username=guest@system
MAC=00-1E-C1-44-47-2E
IP=85.3.1.100
IPv6=N/A
Access=PORTAL  ,AuthMethod=PAP
Port Type=Wireless-802.11,Port Name=Vlan-interface10
Initial VLAN=10, Authorization VLAN=10
ACL Group=3322
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2011-01-30 10:20:03 ,Current=2011-01-30 10:27:19 ,Online=00h07m16s
 Total 1 connection matched.
```

（3）通过ping命令可以验证用户的访问权限，可以看到用户只能访问被授权的地址，其他地址不允许访问。

```
D:\>ping 8.1.1.16
Pinging 8.1.1.16 with 32 bytes of data:
```

```
Reply from 8.1.1.16: bytes=32 time<1ms TTL=254

D:\>ping 8.1.1.20
Pinging 8.1.1.20 with 32 bytes of data:
Reply from 8.1.1.20: bytes=32 time<1ms TTL=254

D:\>ping 8.1.1.22
Pinging 8.1.1.22 with 32 bytes of data:
Request timed out.
Request timed out.
```