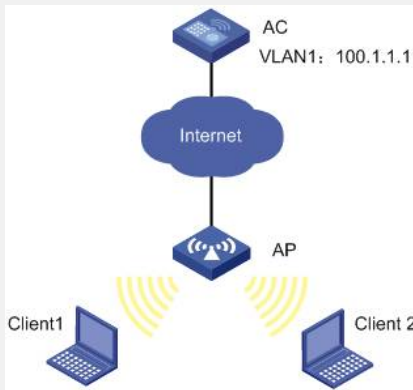


WX系列AC实现Guest-vlan功能的配置

一、组网需求:

WX系列AC、FIT AP、交换机、便携机 (安装有无线网卡)

二、组网图:



本例中AC采用WX3024。

三、特性介绍:

Guest VLAN功能用来允许未认证用户访问某些特定资源。

用户认证端口在通过认证之前属于一个缺省VLAN (即Guest VLAN)，用户访问该VLAN内的资源不需要认证，但此时不能够访问其他网络资源；认证成功后，端口离开Guest VLAN，用户可以访问其他的网络资源。

本特性提供了一种授权属性规划的方法，对于未通过认证或者被定义为临时用户的权限，通过认证的方法予以区别对待，既保证了安全，又非常友好的保证了访问的权限。

四、配置信息:

```
#
version 5.20, Release 3111P10
#
sysname H3C
#
domain default enable system
#
telnet server enable
#
port-security enable
#
dot1x authentication-method eap
#
wlan auto-ap enable
#
vlan 1
#
vlan 2
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
dhcp server ip-pool vlan1
network 100.1.1.0 mask 255.255.255.0
```

```
gateway-list 100.1.1.1
#
dhcp server ip-pool vlan2
network 192.168.2.0 mask 255.255.255.0
gateway-list 192.168.2.1
#
user-group system
user-group eap
local-user admin
password simple admin
authorization-attribute level 3
service-type telnet
local-user eap
password simple eap
group eap
service-type lan-access
#
wlan rrm
dot11a mandatory-rate 6 12 24
dot11a supported-rate 9 18 36 48 54
dot11b mandatory-rate 1 2
dot11b supported-rate 5.5 11
dot11g mandatory-rate 1 2 5.5 11
dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 1 clear
ssid host-guest
bind WLAN-ESS 1
service-template enable
#
eap-profile eap
method md5
#
interface NULL0
#
interface Vlan-interface1
ip address 100.1.1.1 255.255.255.0
#
interface Vlan-interface2
ip address 192.168.2.1 255.255.255.0
#
interface M-GigabitEthernet2/0/0
#
interface Ten-GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan all
#
interface WLAN-ESS1
port link-type hybrid
port hybrid vlan 1 to 2 untagged
port hybrid pvid vlan 1
mac-vlan enable
port-security port-mode userlogin-secure-ext
dot1x guest-vlan 2
#
wlan ap ap model WA2100
serial-id auto
radio 1
#
wlan ap ap_001 model WA2100
serial-id 210235A22WC07C000578
radio 1
service-template 1
radio enable
```

```
#
dhcp enable
#
local-server authentication eap-profile eap
#
load xml-configuration
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
#
user-interface aux 0
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
#
return
```

五、主要配置步骤：

开启端口安全

```
[H3C]port-security enable
```

配置无线接口，端口类型配置成hybrid口，并开启mac-vlan功能

```
[H3C]interface wlan-ess 1
[H3C-WLAN-ESS3] port link-type hybrid
[H3C-WLAN-ESS3] port hybrid vlan 1 to 2 untagged
[H3C-WLAN-ESS3] port hybrid pvid vlan 1
[H3C-WLAN-ESS3] mac-vlan enable
```

配置接口采用802.1X认证方式，并开启Guest vlan功能。

```
[H3C-WLAN-ESS3] port-security port-mode userlogin-secure-ext
[H3C-WLAN-ESS3] dot1x guest-vlan 2
```

配置无线服务模板

```
[H3C]wlan service-template 1 clear
[H3C-wlan-st-3]ssid host-guest
[H3C-wlan-st-3]bind wlan-ess 1
[H3C-wlan-st-3]service-template enable
[H3C-wlan-st-3]quit
```

配置dot1x认证为eap方式，并使能端口安全

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

配置本地认证方式为md5，并使能本地认证服务

```
[AC]eap-profile eap
[AC-eap-prof-eap]method md5
[AC]local-server authentication eap-profile eap
```

创建用户组

```
[AC]user-group eap
```

创建本地用户，服务类型为lan-access

```
[AC]local-user eap
[AC]password simple eap
[AC]group eap
[AC]service-type lan-access
```

六、结果验证：

无线客户端关联到该无线网络，使用iNode客户端登录，输入本地的用户名和密码（本例中用户名和密码均为eap），把iNode上的配置项“携带版本号”勾掉，不要携带版本号进行认证。

当采用正确帐号“eap”认证后，通过命令“display wlan client verbose”查看STA所属VLAN属性如下：

```
[H3C] display wlan client verbose
Total Number of Clients      : 1
Total Number of Clients Connected : 1
Client Information
-----
MAC Address      : 0012-f0cc-3a2c
AID              : 1
Radio Interface  : WLAN-Radio1/0/2
SSID             : host-guest
BSSID           : 000f-e250-22e0
Port             : WLAN-DBSS1: 0
VLAN             : 1
State            : Running
... ..
-----
```

当采用错误帐号（例如“eap2”）时，通过命令“display wlan client verbose”查看STA所属VLAN属性如下：

```
[H3C] display wlan client verbose
Total Number of Clients      : 1
Total Number of Clients Connected : 1
Client Information
-----
MAC Address      : 0012-f0cc-3a2c
AID              : 1
Radio Interface  : WLAN-Radio1/0/2
SSID             : host-guest
BSSID           : 000f-e250-22e0
Port             : WLAN-DBSS1: 0
VLAN             : 2
State            : Running
... ..
-----
```