

知 V7 无线802.1X Fail VLAN 典型配置

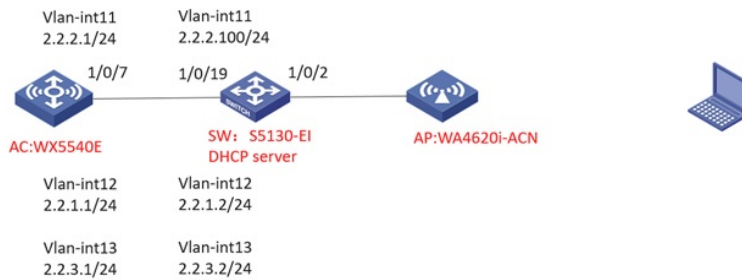
802.1X

wlan优化

陈启敏

2021-01-31 发表

组网及说明



组网需求

1、 如上图所示，sw作为dhcp server 为ap和client分配地址，要求：

- l 对无线用户进行本地802.1x认证
- l 认证失败后访问某一特定vlan auth-fail vlan的资源

特性介绍：802.1X Auth-Fail VLAN功能允许用户在认证失败的情况下访问某一特定VLAN中的资源，这个VLAN称之为Auth-Fail VLAN。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。根据端口的接入控制方式不同，Auth-Fail VLAN的生效情况有所不同。

配置步骤

配置步骤

配置AC

(1) 配置AC的接口

#创建vlan 11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

```
system-view
[AC] vlan 11
[AC-vlan11] quit
[AC] interface vlan-interface 11
[AC-Vlan-interface11] ip address 2.2.2.1 24
[AC-Vlan-interface11] quit
# 创建VLAN 12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 12
[AC-vlan12] quit
[AC] interface vlan-interface 12
[AC-Vlan-interface12] ip address 2.2.1.1 24
[AC-Vlan-interface12] quit
# 创建VLAN 13及其对应的VLAN接口，并为该接口配置IP地址。Client dot1x接入失败后可访问该VLAN中的资源。该VLAN为fail-vlan.
[AC] vlan 13
[AC-vlan13] quit
[AC] interface vlan-interface 13
[AC-Vlan-interface13] ip address 2.2.3.1 24
[AC-Vlan-interface13] quit

# 在1/0/7接口下配置fail vlan 13
[AC] int 1/0/7
[AC] dot1x auth-fail vlan 13
```

配置Switch与AC相连的GigabitEthernet1/0/7接口的属性为Trunk，允许VLAN 11和VLAN 12、vlan13通过。

```
[AC] interface gigabitethernet 1/0/7
[AC-GigabitEthernet1/0/7] port link-type trunk
[AC-GigabitEthernet1/0/7] port trunk permit vlan 11 12 13
[AC-GigabitEthernet1/0/7] quit
```

(2) 配置本地用户

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

```
[AC] local-user cqmfailvlan class network
[AC-luser-network- cqmfailvlan] password simple cqmfailvlanpass
# 配置本地用户的服务类型为lan-access。
[AC-luser-network-l cqmfailvlan] service-type lan-access
[AC-luser-network cqmfailvlan] quit
```

(3) 配置ISP域

创建名为cqm的ISP域并进入其视图。

```
[AC] domain cqm
# 为802.1X用户配置AAA认证方法为本地认证、授权和计费。
[AC-isp-cqm] authentication lan-access local
[AC-isp-cqm] authorization lan-access local
[AC-isp-cqm] accounting lan-access local
[AC-isp-cqm] 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service1，并进入无线服务模板视图。

```
[AC] wlan service-template service1
# 配置SSID为servicecqm。
[AC-wlan-st-service1] ssid servicecqm
# 配置无线服务模板VLAN为12。
[AC-wlan-st-service1] vlan 12
# 配置用户接入认证模式为802.1X。
[AC-wlan-st-service1] client-security authentication-mode dot1x
[AC-wlan-st-service1] client-security authentication fail-vlan 13
# 配置802.1X用户使用认证域为cqm。
```

```
[AC-wlan-st-service1] dot1x domain cqm
```

```
# 使能无线服务模板。
```

```
[AC-wlan-st-service1] service-template enable
```

```
[AC-wlan-st-service1] quit
```

配置关键点

```
# 创建AP，配置AP名称为cqmtest，型号名称选择WA4320i-ACN，并配置序列号210235A1GQ
```

```
C158004457。
```

```
[AC] wlan ap cqmtest model WA4620i-ACN
```