基于SSID的mac认证配置

wlan接入 MAC地址认证 User Profile **殷俊** 2016-04-25 发表

基于SSID绑定mac认证，指定用户通过mac认证接入指定SSID

配置思路：

1. 创建两个user-profile分别命名为linc /linc1,分别绑定SSID为linc/linc1，并使能user-profile XXX enable
2. 创建mac认证用的用户名信息local-user 48746e28396f/ c0f2fbd80ca6分别绑定对应的user-profile：authorization-attribute user-profile linc/linc1
3. 创建服务模板，配置对应的SSID

配置完成后，终端A只能通过mac认证关联SSID linc，终端B只能通过mac认证关联SSID linc1

关键配置如下标红部分：

dis cu

```
#
 version 5.20, Release 3509P41
#
 sysname WX3010E
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
 mac-authentication domain system
#
 oap management-ip 192.168.0.101 slot 0
#
 wlan auto-ap enable
#
 password-recovery enable
#
vlan 1
#
vlan 10
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool vlan10
 network 10.0.0.0 mask 255.255.255.0
 gateway-list 10.0.0.1
#
user-group system
 group-attribute allow-guest
#
local-user 48746e28396f
 password cipher $c$3$8oC2hGF9B8qdDvgqKPvtIgGRx9JkSYpJoHgHHiEBaA==
 authorization-attribute user-profile linc1   //mac认证终端绑定user-profile linc1用户组
 service-type lan-access
local-user admin
 password cipher $c$3$2l4Gnxd2YrAZA2vJKwKdiViFMs+7A2e3
 authorization-attribute level 3
 service-type ssh telnet
local-user c0f2fbd80ca6
 password cipher $c$3$swFgTbm9dMIWwBeiELVPVeNqfqy4+u/iLmVOmkp3/Q==
 authorization-attribute user-profile linc    //mac认证终端绑定user-profile linc用户组
 service-type lan-access
local-user linc
 password cipher $c$3$rzZYnbPIgRX+siQjdXjDWEl80/8veJ8=
 authorization-attribute level 3
 service-type ssh
#
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 linc
 bind WLAN-ESS 1
 service-template enable
#
wlan service-template 2 clear
 ssid linc1
 bind WLAN-ESS 2
 service-template enable
#
wlan ap-group default_group
 ap ap1
 ap 80f6-2e4d-4540
#
user-profile linc
 wlan permit-ssid linc   // user-profile linc用户组绑定SSID信息
user-profile linc1
 wlan permit-ssid linc1  // user-profile linc1用户组绑定SSID信息
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface10
 ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface WLAN-ESS1
 port access vlan 10
 port-security port-mode mac-authentication
#
interface WLAN-ESS2
 port access vlan 10
 port-security port-mode mac-authentication
#
wlan ap 80f6-2e4d-4540 model WA4620i-ACN id 2
 serial-id 210235A1BSC145001796
 radio 1
  service-template 1
  service-template 2
  radio enable
 radio 2
#
wlan ap ap1 model WA4620i-ACN id 1
 serial-id auto
 radio 1
 radio 2
#
wlan ips
 malformed-detect-policy default
```

```
 signature deauth_flood signature-id 1
 signature broadcast_deauth_flood signature-id 2
 signature disassoc_flood signature-id 3
 signature broadcast_disassoc_flood signature-id 4
 signature eapol_logoff_flood signature-id 5
 signature eap_success_flood signature-id 6
 signature eap_failure_flood signature-id 7
 signature pspoll_flood signature-id 8
 signature cts_flood signature-id 9
 signature rts_flood signature-id 10
 signature addba_req_flood signature-id 11
 signature-policy default
 countermeasure-policy default
 attack-detect-policy default
 virtual-security-domain default
  attack-detect-policy default
  malformed-detect-policy default
  signature-policy default
  countermeasure-policy default
#
 dhcp enable
#
 ssh server enable
 ssh user linc service-type stelnet authentication-type password
#
 user-profile linc enable
 user-profile linc1 enable
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
 protocol inbound ssh
#
return
```