基于MAC认证的Portal无感知认证：基于portal在线用户的MAC认证

王森森 2014-06-05 发表

基于MAC认证的Portal无感知认证：基于portal在线用户的MAC认证

一、组网需求：

WX系列AC、FIT AP、便携机（安装有无线网卡）、Radius/Portal Server

二、实现原理：

中国移动主推的Portal无感知认证是基于流量触发的mac-trigger，要求支持移动的mac-trigger协议，并且新增MAC绑定服务器以存储MAC的绑定关系。对于第三方的Radius/Portal server厂商来说开发较繁琐，有些厂商是不支持的。如果不支持mac-trigger协议，可以以下方案实现Portal的无感知认证，实现原理如下：

（1）用户的业务VLAN开启MAC认证和guest vlan功能；

（2）用户第一次上线时进行MAC认证，AC根据用户MAC查找在线Portal用户，如果有该MAC地址的Portal用户，则MAC认证成功。因为用户第一次认证，AC没有该MAC地址的Portal在线用户，用户MAC认证失败，进入guest vlan；

（3）guest vlan开启Portal认证；

（4）用户在guest vlan进行Portal认证，Portal认证成功后，AC立即将该用户去关联，触发用户重关联，此时由于设置idle-cut时间还未生效，AC上有该Portal用户在线；

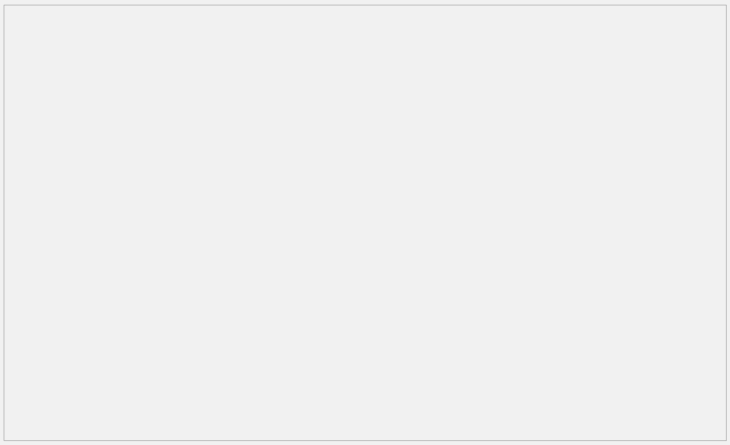
（5）用户重关联时进行MAC认证，此时AC上已有该MAC地址的Portal用户，MAC认证通过。

（6）用户后续都是无感知的MAC认证，MAC认证通过的前提是对应MAC地址的Portal用户在线，因为后续用户流量属于业务VLAN，Portal用户的流量为0，因此设置idle-cut时间为Portal用户的在线时间，即用户能够MAC认证通过的时间。

备注：

该方案中，第三方Radius/Portal server只需具有Radius服务器和Portal服务器的功能，没有特殊要求，基于portal用户的MAC认证功能在AC自身实现。

三、组网图：



本典型配置举例中AC使用WX5004无线控制器，版本为R2507P18。SW作为AP网关（Vlan-int2：192.168.2.254/24）、Client进行MAC认证的vlan网关（Vlan-int10：192.168.10.254/24）、Client进行Portal认证的guest vlan网关（Vlan-int11：192.168.11.254/24），并配置DHCP Server为FIT AP、Client分配IP地址。第三方Radius/Portal server的IP地址为192.168.100.253，AC通过IP地址192.168.100.1与其互联。

四、配置信息：

1．AC配置信息：

```
#
 version 5.20, Release 2507P18
#
 sysname AC
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
 portal server dsf-portal ip 192.168.100.253 key cipher $c$3$uDGtFFtWMQH6VTGb
```

```
Bg3tVMYIv+F00w== url http://192.168.100.253/portal server-type imc
 portal free-rule 0 source mac 3822-d6c0-ad73 destination any
#
vlan 1
#
vlan 2
#
vlan 10 to 11
#
Vlan 100
#
vlan 1000
#
radius scheme dsf-portal
 primary authentication 192.168.100.253
 primary accounting 192.168.100.253
 key authentication cipher $c$3$o1jrlBnKIVhr5s6BS5Ck3pV2XGtpFQ==
 key accounting cipher $c$3$JvB3TU6DkwokktR2uX/6vl5S+5XWvg==
 user-name-format without-domain
 nas-ip 192.168.100.1
#
domain dsf-mac
 authentication lan-access none
 authorization lan-access none
 accounting lan-access none
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain dsf-portal
 authentication portal radius-scheme dsf-portal
 authorization portal none
 accounting portal none
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher $c$3$4CSnRqvYBd2xHeUsyDKNVbcG7cL1Q/IT
 authorization-attribute level 3
 service-type telnet
#
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 dsf-portal
 bind WLAN-ESS 1
 service-template enable
#
```

```
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface2
 ip address 192.168.2.1 255.255.255.0
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface11
 ip address 192.168.11.1 255.255.255.0
 portal server dsf-portal method direct
 portal domain dsf-portal
 portal nas-port-type wireless
 portal nas-ip 192.168.100.1
#
interface Vlan-interface100
 ip address 192.168.100.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
#
interface Ten-GigabitEthernet1/0/5
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1000 untagged
 port hybrid pvid vlan 1000
 mac-vlan enable
port-security port-mode mac-authentication
 mac-authentication guest-vlan 11
 mac-authentication domain dsf-mac
 mac-authentication trigger after-portal
#
wlan ap ap01 model WA2220-AG id 1
 serial-id 210235A29EB092002600
 radio 1
  service-template 1 vlan-id 10
  radio enable
 radio 2
  service-template 1 vlan-id 10
  radio enable
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.100.254
#
 undo info-center logfile enable
#
 snmp-agent
 snmp-agent local-engineid 800063A2033CE5A684342E
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
#
 arp-snooping enable
```

```
#
 load xml-configuration
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

2．SW的配置信息：

```
#
 version 5.20, Release 2103
#
 sysname SW
#
 domain default enable system
#
 telnet server enable
#
vlan 1
#
vlan 2
#
vlan 10 to 11
#
vlan 100
#
radius scheme system
 server-type extended
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool pool-ap
 network 192.168.2.0 mask 255.255.255.0
 gateway-list 192.168.2.254
#
dhcp server ip-pool pool-client-mac
 network 192.168.10.0 mask 255.255.255.0
 gateway-list 192.168.10.254
#
dhcp server ip-pool pool-client-portal
 network 192.168.11.0 mask 255.255.255.0
 gateway-list 192.168.11.254
#
user-group system
 group-attribute allow-guest
#
local-user admin
#
interface NULL0
#
interface Vlan-interface2
 ip address 192.168.2.254 255.255.255.0
#
interface Vlan-interface10
 ip address 192.168.10.254 255.255.255.0
#
```

```
interface Vlan-interface11
 ip address 192.168.11.254 255.255.255.0
#
interface Vlan-interface100
 ip address 192.168.100.254 255.255.255.0
#
interface Ethernet1/0/1
 port link-mode bridge
 port access vlan 2
 poe enable
#
interface Ethernet1/0/23
 port link-mode bridge
 port access vlan 100
#
interface Ethernet1/0/24
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
#
 dhcp server forbidden-ip 192.168.2.1
 dhcp server forbidden-ip 192.168.10.1
dhcp server forbidden-ip 192.168.11.1
#
 dhcp enable
#
 load xml-configuration
#
 load tr069-configuration
#
user-interface aux 0
user-interface vty 0 15
#
return
```

五、主要配置步骤：

1．AC配置：

#创建VLAN，二层端口配置VLAN信息，并配置VLAN接口IP地址。

```
<AC> system-view
[AC] vlan 2
[AC –vlan2] quit
[AC] vlan 10
[AC –vlan10] quit
[AC] vlan 11
[AC –vlan11] quit
[AC] vlan 100
[AC –vlan100] quit
[AC] vlan 1000
[AC –vlan1000] quit
[AC] interface GigabitEthernet1/0/1
[AC- GigabitEthernet1/0/1] port link-type trunk
[AC- GigabitEthernet1/0/1] port trunk permit vlan all
[AC] interface Vlan-interface2
[AC-Vlan-interface2] ip address 192.168.2.1 255.255.255.0
[AC-Vlan-interface2] quit
[AC] interface Vlan-interface10
[AC-Vlan-interface10] ip address 192.168.10.1 255.255.255.0
[AC-Vlan-interface10] quit
[AC] interface Vlan-interface11
[AC-Vlan-interface11] ip address 192.168.11.1 255.255.255.0
[AC-Vlan-interface11] quit
[AC] interface Vlan-interface100
[AC-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
[AC-Vlan-interface100] quit
```

#使能ARP Snooping功能，命令display wlan client显示无线客户端的IP地址。

[AC] arp-snooping enable
#配置静态路由。
[AC] ip route-static 0.0.0.0 0.0.0.0 192.168.100.254
配置RADIUS方案，创建名称为dsf-mac的RADIUS方案。
[AC] radius scheme dsf-mac
#配置MAC认证域，创建并进入名字为dsf-mac的ISP域。
[AC] domain dsf-mac
[AC-isp- dsf-mac] authentication lan-access none
[AC-isp- dsf-mac] authorization lan-access none
[AC-isp- dsf-mac] accounting lan-access none
[AC-isp- dsf-mac] quit
配置Portal认证RADIUS方案，创建名称为dsf-portal的RADIUS方案。
[AC] radius scheme dsf-portal
[AC-radius- dsf-portal] primary authentication 192.168.100.253
[AC-radius- dsf-portal] primary accounting 192.168.100.253
[AC-radius- dsf-portal] key authentication dsf
[AC-radius- dsf-portal] key accounting dsf
[AC-radius- dsf-portal] user-name-format without-domain
[AC-radius- dsf-portal] nas-ip 192.168.100.1
[AC-radius- dsf-portal] quit
#配置Portal认证域，创建并进入名字为dsf-portal的ISP域。
[AC] domain dsf-portal
[AC-isp- dsf-portal] authentication portal radius-scheme dsf-portal
[AC-isp- dsf-portal] authorization portal none
[AC-isp- dsf-portal] accounting portal none
[AC-isp- dsf-portal] quit
#配置Portal服务器：名称为dsf-portal，IP地址为192.168.100.253，密钥为dsf，URL为http://192.168.100.253/portal。
[AC] portal server dsf-portal ip 192.168.100.253 key dsf url
http://192.168.100.253/portal server-type imc
#配置Portal free-rule，允许源MAC 地址为用户网关MAC（3822-d6c0-ad73）的所有流量。
[AC] portal free-rule 0 source mac 3822-d6c0-ad73 destination any
#在用户MAC认证guest vlan接口上使能Portal认证，并配置接入的Portal用户使用认证域dsf-portal。
[AC] interface Vlan-interface11
[AC-Vlan-interface11] portal server dsf-portal method direct
[AC-Vlan-interface11] portal domain dsf-portal
[AC-Vlan-interface11] portal nas-port-type wireless
[AC-Vlan-interface11] portal nas-ip 192.168.100.1
[AC-Vlan-interface11] quit
#配置端口安全。
[AC] port-security enable
#配置WLAN ESS接口，并配置MAC认证。
[AC] interface WLAN-ESS1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 1000 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 1000
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] port-security port-mode mac-authentication
[AC-WLAN-ESS1] mac-authentication guest-vlan 11
[AC-WLAN-ESS1] mac-authentication domain dsf-mac
#指定对用户的MAC地址认证必须在该用户通过Portal认证之后。
[AC-WLAN-ESS1] mac-authentication trigger after-portal
[AC-WLAN-ESS1]quit
#配置service-template服务模板。
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid dsf-portal
[AC-wlan-st-1] bind WLAN-ESS 1
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
#配置ap1。
[AC] wlan ap ap01 model WA2220-AG

[AC-wlan-ap-ap01] serial-id 210235A29EB092002600
[AC-wlan-ap-ap01] radio 1
[AC- wlan-ap-ap01-radio-1] service-template 1 vlan-id 10
[AC- wlan-ap-ap01-radio-1] radio enable
[AC- wlan-ap-ap01-radio-1] quit
[AC-wlan-ap-ap01] radio 2
[AC- wlan-ap-ap01-radio-2 service-template 1 vlan-id 10
[AC- wlan-ap-ap01-radio-2 radio enable
[AC- wlan-ap-ap01-radio-2 quit
[AC-wlan-ap-ap01] quit
#配置SNMP。
[AC] snmp-agent
[AC] snmp-agent community read public
[AC] snmp-agent community write private
[AC] snmp-agent sys-info version all
2．SW配置：
#创建VLAN，二层端口配置VLAN信息，并配置VLAN接口IP地址。
<SW> system-view
[SW] vlan 2
[SW –vlan2] quit
[SW] vlan 10
[SW –vlan10] quit
[SW] vlan 11
[SW –vlan11] quit
[SW] vlan 100
[SW –vlan100] quit
[SW] interface Ethernet1/0/1
[SW-Ethernet1/0/1] port access vlan 2
[SW-Ethernet1/0/1] poe enable
[SW-Ethernet1/0/1] quit
[SW] interface Ethernet1/0/23
[SW-Ethernet1/0/23] port access vlan 100
[SW-Ethernet1/0/23] quit
[SW] interface Ethernet1/0/24
[SW-Ethernet1/0/24] port link-type trunk
[SW-Ethernet1/0/24] port trunk permit vlan all
[SW-Ethernet1/0/24] quit
[SW] interface Vlan-interface2
[SW-Vlan-interface2] ip address 192.168.2.254 255.255.255.0
[SW-Vlan-interface2] quit
[SW] interface Vlan-interface10
[SW-Vlan-interface10] ip address 192.168.10.254 255.255.255.0
[SW-Vlan-interface10] quit
[SW] interface Vlan-interface11
[SW -Vlan-interface11] ip address 192.168.11.254 255.255.255.0
[SW -Vlan-interface11] quit
[SW] interface Vlan-interface100
[SW -Vlan-interface100] ip address 192.168.100.254 255.255.255.0
[SW -Vlan-interface100] quit
#配置DHCP server。
[SW] dhcp enable
[SW] dhcp server ip-pool pool-ap
[SW- dhcp server ip-pool pool-ap] network 192.168.2.0 mask 255.255.255.0
[SW- dhcp server ip-pool pool-ap] gateway-list 192.168.2.254
[SW- dhcp server ip-pool pool-ap] quit
[SW] dhcp server ip-pool pool-client-mac
[SW- dhcp server ip-pool pool-client-mac] network 192.168.10.0 mask 255.255.255.0
[SW- dhcp server ip-pool pool-client-mac] gateway-list 192.168.10.254
[SW- dhcp server ip-pool pool-client-mac] quit
[SW] dhcp server ip-pool pool-client-portal
[SW- dhcp server ip-pool pool-client-portal] network 192.168.11.0 mask
255.255.255.0
[SW- dhcp server ip-pool pool-client-portal] gateway-list 192.168.11.254
[SW- dhcp server ip-pool pool-client-portal] quit

[SW] dhcp server forbidden-ip 192.168.2.1
[SW] dhcp server forbidden-ip 192.168.10.1
[SW] dhcp server forbidden-ip 192.168.11.1

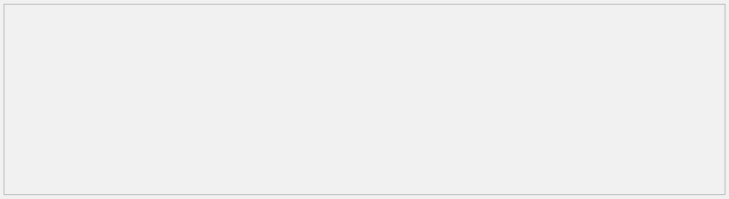
3．第三方Radius/Portal server配置：

第三方Radius/Portal server只需具有Radius服务器和Portal服务器的功能，没有特殊要求，基于portal用户的MAC认证功能在AC自身实现。

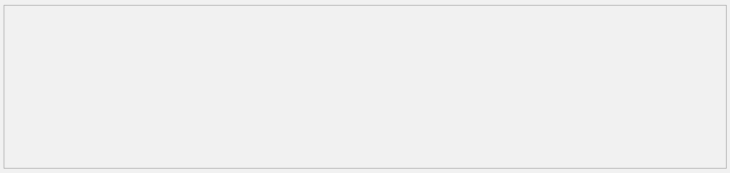
六、结果验证：

（1）Client首次接入无线服务，MAC认证未通过，进入Guest VLAN11。

（2）Client通过浏览器访问网络，弹出认证页面，输入用户名密码后，Portal认证通过，通过display portal user all命令查看存在Portal用户信息。



（3）AC将该Client下线，重新接入该服务，MAC认证成功，Client进入VLAN 10。



（4）在AC上通过display connection命令查看在线用户信息，存在MAC认证和Portal认证2个用户。此时Client可以通过业务网关访问Internet网络。