WX系列AC结合iMC进行Portal认证实现终端识别的配置（Radius属性方式）

Portal AAA wlan接入 DHCP c09467 2014-04-29 发表

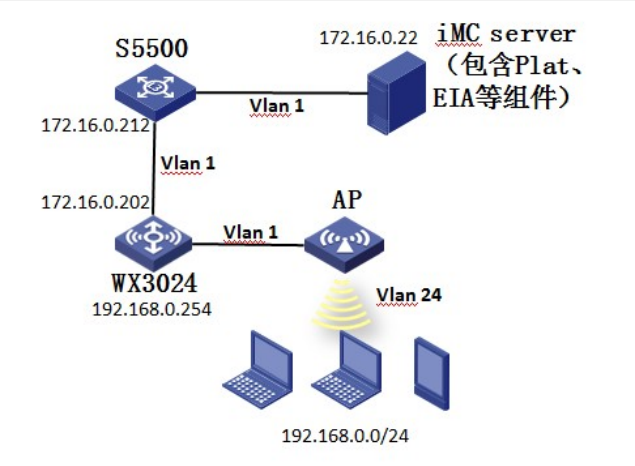
WX系列AC结合iMC进行Portal认证实现终端识别的配置（Radius属性方式）

一、 组网需求：

在BYOD组网方案下，我们主要通过iNode客户端、HTTP网页、终端Mac地址以及DHCP的Option属性这四种方式获取终端的操作系统和厂商信息，实现终端识别以便完成相应的权限策略控制。其中DHCP的Option属性方式可普遍用户各种场景。由于部署DHCP服务器并安装Agent插件的方式比较繁琐，这里我们以普通Portal认证为例介绍一种通过无线控制器的DHCP-snooping功能获取记录终端的option 55（终端操作系统）和option 60（终端厂商）信息并通过Radius属性上报给iMC服务器的典型配置。

WX系列AC、Fit AP、交换机、便携机（安装有无线网卡）、iMC服务器及其他智能终端。

二、 组网图：



三、 配置步骤：

1、 AC版本要求

WX系列AC从B109D012合入该特性，因此只有这个版本号及其以后的版本支持DHCP-snooping功能获取记录终端的option 55（终端操作系统）和option 60（终端厂商）信息并通过Radius属性上报给iMC服务器。WX系列AC可通过下面的命令查看内部版本号：

_display version

H3C Comware Platform Software

Comware Software, Version 5.20, Release 2607P18

Comware Platform Software Version COMWAREV500R002B109D022

H3C WX5540E Software Version V200R006B09D022

Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.

Compiled Feb 25 2014 11:08:07, RELEASE SOFTWARE

H3C WX5540E uptime is 1 week, 4 days, 0 hour, 49 minutes

2、 AC侧配置及说明

#

version 5.20, Release 3120P17

#

sysname WX3024-AC

#

domain default enable system

#

```
 telnet server enable
#
 port-security enable
#
      //配置portal server、ip、key、url以及server-type，注意这里server-type必须配置为imc
      portal server imc ip 172.16.0.22 key cipher $c$3$6uB5v4kaCg1aSOJkOqX+== url htt
      p://172.16.0.22:8080/portal server-type imc
//配置portal free-rule放通AC内联口
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
#
 oap management-ip 192.168.0.101 slot 0
#
 password-recovery enable
#
vlan 1
#
vlan 24
#
     //配置radius策略，注意server-type必须选择extended模式，注意user-name-format及nas-ip的配置
     必须与iMC接入策略和接入服务里配置保持一致。
radius scheme imc
 server-type extended
 primary authentication 172.16.0.22
 primary accounting 172.16.0.22
 key authentication cipher $c$3$Myv0nhgPjC4vsMforZW3iCiW5KkP7Q==
 key accounting cipher $c$3$dCEXJGp71WPyrPK4hsPJd6sdTYf01A==
 user-name-format without-domain
 nas-ip 172.16.0.202
#
//配置domain
domain imc
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
 accounting portal radius-scheme imc
 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
#
//配置AP注册dhcp pool
dhcp server ip-pool 1
```

```
 network 192.168.0.0 mask 255.255.255.0
#
//配置终端业务dhcp pool
dhcp server ip-pool option55
 network 192.168.24.0 mask 255.255.255.0
 gateway-list 192.168.24.254
 dns-list 8.8.8.8
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher $c$3$iMGlwEx7o4TNbMqd7OaOAwB5SWSzOrKE
 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
#
//配置无线服务模板
wlan service-template 10 clear
 ssid option55
 bind WLAN-ESS 10
 service-template enable
#
wlan ap-group default_group
 ap ap1
 ap ap2
#
interface NULL0
#
//与iMC互联ip及vlan接口
interface Vlan-interface1
 ip address 172.16.0.202 255.255.255.0
#
      //终端业务互联ip及vlan接口，接口下开启portal，注意portal domain及portal nas-ip配置需要与iMC服务器portal设备保持一致
interface Vlan-interface24
 ip address 192.168.24.1 255.255.255.0
 portal server imc method direct
 portal domain imc
```

```
 portal nas-ip 172.16.0.202
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
//配置wlan-ess接口
interface WLAN-ESS10
 port access vlan 24
#
wlan ap ap2 model WA2610H-GN id 2
 serial-id 219801A0FH9136Q00287
 radio 1
  service-template 10
  radio enable
#
       //开启dhcp-snooping，使能dhcp-snooping记录用户的option 55和option 60信息功能
dhcp-snooping
dhcp-snooping binding record user-identity
#
//配置默认路由
 ip route-static 0.0.0.0 0.0.0.0 192.168.24.254
#
 snmp-agent
 snmp-agent local-engineid 800063A203000FE2873066
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
#
//使能dhcp
dhcp enable
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

3、 iMC侧配置请参考KMS-21434《 WX系列AC与iMC配合实现无线Portal认证典型配置》，这里不再赘述。

4、 结果验证及抓包

1）AC上查看在线的客户端和portal在线用户信息：

```
dis wlan client
 Total Number of Clients           : 2
                          Client Information
 SSID: option55
```

MAC Address User Name APID/RID IP Address VLAN

2477-0391-7720 -NA- 2/1 192.168.24.2 24

28e1-4cb5-8249 -NA- 2/1 192.168.24.3 24

---

dis portal user all

Index:12

State:ONLINE

SubState:NONE

ACL:NONE

Work-mode:stand-alone

MAC IP Vlan Interface

2477-0391-7720 192.168.24.2 24 Vlan-interface24

Index:13

State:ONLINE

SubState:NONE

ACL:NONE

Work-mode:stand-alone

MAC IP Vlan Interface

28e1-4cb5-8249 192.168.24.3 24 Vlan-interface24

Total 2 user(s) matched, 2 listed.

2）iMC上通过终端设备管理查看终端的厂商、类型以及操作系统等信息：

3）查看AC的debugging信息，可以清楚看到Radius的code=[1]报文里携带了option 55和option 60的属性字段：

*Apr 26 16:37:06:936 2000 WX3024-AC RDS/7/DEBUG: Send attribute list:

*Apr 26 16:37:06:946 2000 WX3024-AC RDS/7/DEBUG:

[1 User-name] [8] [c09467]

[60 CHAP_Challenge] [18] [6EFCA7E2624584E38EA53882A4A12C90]

[4 NAS-IP-Address] [6] [172.16.0.202]

[32 NAS-Identifier] [11] [WX3024-AC]

[5 NAS-Port] [6] [16818200]

[87 NAS_Port_Id] [18] [0100010000000024]

*Apr 26 16:37:06:986 2000 WX3024-AC RDS/7/DEBUG:

[61 NAS-Port-Type] [6] [19]

[H3C-26 Connect_ID] [6] [21]

[6 Service-Type] [6] [2]

[7 Framed-Protocol] [6] [255]

[31 Caller-ID] [19] [36432D38382D31342D35392D38392D3843]

[30 Called-station-Id] [28] [74-25-8A-33-81-70:option55]

*Apr 26 16:37:07:027 2000 WX3024-AC RDS/7/DEBUG:

[44 Acct-Session-Id] [16] [10003261637160]

[8 Framed-Address] [6] [192.168.24.4]

[H3C-255Product-ID] [12] [H3C WX3024]

[H3C-60 Ip-Host-Addr] [32] [192.168.24.4 6c:88:14:59:89:8c]

[H3C-208 DHCP-Option55] [14] [010F03062C2E2F1F2179F92B]

[H3C-209 DHCP-Option60] [10] [4D53465420352E30]

*Apr 26 16:37:07:077 2000 WX3024-AC RDS/7/DEBUG:

[H3C-59 NAS-Startup-Timestamp] [6] [956750400]

*Apr 26 16:37:07:087 2000 WX3024-AC RDS/7/DEBUG:

Event: Begin to switch RADIUS server when sending 0 packet.

*Apr 26 16:37:07:108 2000 WX3024-AC RDS/7/DEBUG: The RD TWL timer has resumeed.

%Apr 26 16:37:07:118 2000 WX3024-AC RDS/6/RDS_SUCC: -IfName=Vlan-interface24-VlanId=24-MACAddr=6C:88:14:59:89:8C-IPAddr=192.168.24.4-IPv6Addr=N/A-UserName=c09467@imc; User got online successfully.

%Apr 26 16:37:07:138 2000 WX3024-AC PORTAL/5/PORTAL_USER_LOGON_SUCCESS: -UserName=c09467-IPAddr=192.168.24.4-IfName=Vlan-interface24-VlanID=24-MACAddr=6c88-1459-898c-APMAC=7425-8A33-8170-SSID=option55-NasId=-NasPortId=; User got online successfully.

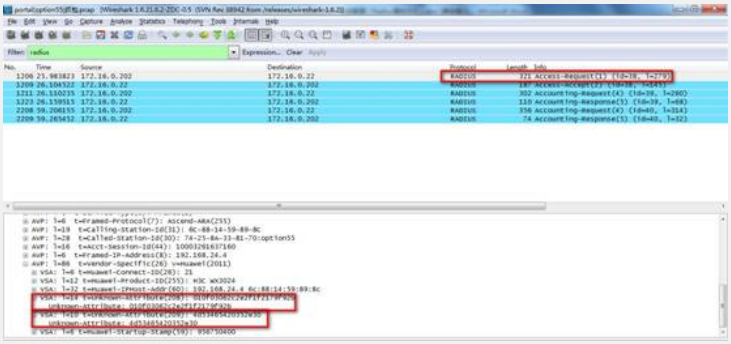
*Apr 26 16:37:07:169 2000 WX3024-AC RDS/7/DEBUG: Malloc seed:38 in 172.16.0.22 for User ID:21

*Apr 26 16:37:07:179 2000 WX3024-AC RDS/7/DEBUG:

Event: Modify NAS-IP to 172.16.0.202.

*Apr 26 16:37:07:189 2000 WX3024-AC RDS/7/DEBUG: Send: IP=[172.16.0.22], UserIndex=[21], ID=[38], RetryTimes=[0], Code=[1], Length=[279]

4）通过抓包我们也可以看到这个属性字段：



四、 配置关键点：

1、portal server的server-type必须选择imc，radius scheme的server-type必须选择extended。

2、全局视图下开启dhcp-snooping和dhcp-snooping binding record user-identity。

3、AC本身并不支持终端操作系统和厂商识别，只是把相关option 55和option 60信息传送给iMC完成终端识别。