AC本地转发+Portal认证典型配置举例（AP做NAT方式）

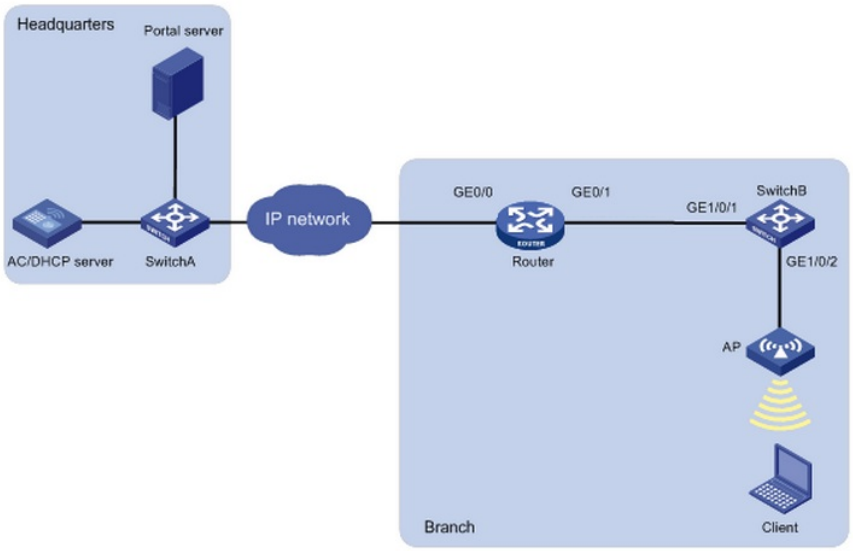
NAT Portal 余晨 2017-03-28 发表

总部的AC与分支机构的AP跨三层关联并作为DHCP server为Client分配IP地址；Router为AP分配IP地址，具体要求如下：

· 用户通过Portal认证接入无线网络；

· 用户通过Portal认证后，AC将用户规则下发到AP上，用户报文在AP上直接做转发。AP三层业务接口配置静态NAT，并将ACL和地址池关联

· 分支节点Router为即插即用简易设备，默认支持DHCP，无需做过多配置。



1、配置Switch A

 # 创建VLAN 10及其对应的VLAN接口，并为该接口配置IP地址，用来和AC通信。

<SwitchA> system-view

[SwitchA] vlan 10

[SwitchA-vlan10] quit

[SwitchA] interface vlan 10

[SwitchA-Vlan-interface10] ip addsress 138.10.1.1 16

[SwitchA-Vlan-interface10] quit

创建VLAN 20及其对应的VLAN接口，并为该接口配置IP地址，用来和AP通信。

[SwitchA] vlan 20

[SwitchA-vlan20] quit

[SwitchA] interface vlan 20

[SwitchA-Vlan-interface20] ip address 138.20.1.1 16

[SwitchA-Vlan-interface20] quit

创建VLAN 30及其对应的VLAN接口，并为该接口配置IP地址，用来和Client通信。

[SwitchA] vlan 30

[SwitchA-vlan30] quit

[SwitchA] interface vlan 30

[SwitchA-Vlan-interface30] ip address 192.168.100.101 16

[SwitchA-Vlan-interface30] quit

#创建VLAN138及其对应的VLAN接口，并为该接口配置IP地址，用来和Portal服务器通信。

[SwitchA] vlan 138

[SwitchA-vlan138] quit

[SwitchA] interface vlan 138

[SwitchA-Vlan-interface138] ip address 8.138.1.2 16

[SwitchA-Vlan-interface138] quit

创建聚合口4。

[SwitchA] interface bridge-aggregation 4

[SwitchA-Bridge-Aggregation4] quit

配置SwitchA与AC连接的接口加入聚合口4。

[SwitchA] interface ten-gigabitethernet 4/0/1
[SwitchA-Ten-GigabitEthernet4/0/1] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/1] quit
[SwitchA] interface ten-gigabitethernet 4/0/2
[SwitchA-Ten-GigabitEthernet4/0/2] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/2] quit
配置聚合口为Trunk口，并允许所有VLAN通过。
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan all
[SwitchA-Bridge-Aggregation4] quit
配置静态路由，用于AC与Portal服务器通信，下一跳指向与Portal服务器互通的网关。
[SwitchA] ip route-static 8.0.0.0 8 8.138.1.1

2、配置AC

(1)　配置AC接口

#创建VLAN 10及其对应的VLAN接口，并为该接口配置IP地址，用来和Portal服务器通信。
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 138.10.1.80 255.255.0.0
[AC-Vlan-interface10] quit
创建VLAN 30及其对应的VLAN接口，并为该接口配置IP地址，用来进行Portal认证。
[AC] vlan 30
[AC-vlan30] quit
[AC] interface vlan-interface 30
[AC-Vlan-interface30] ip address 192.168.100.100 255.255.0.0
[AC-Vlan-interface30] quit
创建聚合口1。
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] quit
将AC上两个物理口加入聚合口1。
[AC] interface ten-gigabitethernet 1/0/1
[AC-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
[AC-Ten-GigabitEthernet1/0/1] quit
[AC] interface ten-gigabitethernet 1/0/2
[AC-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
[AC-Ten-GigabitEthernet1/0/2] quit
配置AC聚合口1的类型为Trunk口并允许所有VLAN通过，用来和AP、Client通信。
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] port link-type trunk
[AC-Bridge-Aggregation1] port trunk permit vlan all
[AC-Bridge-Aggregation1] quit

(2)　配置DHCP服务

使能DHCP功能。
[AC] dhcp enable
#配置DHCP地址池30，为Client动态分配地址，并将网关指向AP的vlan-interface 30。
[AC] dhcp server ip-pool 30
[AC-dhcp-pool-10] network 192.168.0.0 16
[AC-dhcp-pool-10] gateway-list 192.168.1.1
[AC-dhcp-pool-10] dns-list 8.1.1.50
[AC-dhcp-pool-10] quit

(3)　配置WLAN-ESS接口

创建接口WLAN-ESS 30。
[AC] interface wlan-ess 30
配置端口的链路类型为Access，允许VLAN 30通过。
[AC-WLAN-ESS30] port access vlan 30
[AC-WLAN-ESS30] quit

(4)　配置无线服务模板

创建clear类型的无线服务模板service1。
[AC] wlan service-template service1 clear
设置当前服务模板的SSID为portal-local。
[AC-wlan-st-service1] ssid portal-local
将WLAN-ESS30接口绑定到无线服务模板service1。

[AC-wlan-st-service1] bind wlan-ess 30
开启用户本地转发功能。
[AC-wlan-st-service1] client forwarding-mode local
开启无线客户端透传DHCP报文到AC的功能。
[AC-wlan-st-service1] client dhcp-server centralized
使能无线服务模板。
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
(5)　在AC下绑定无线服务模板
创建AP模板，名称为ap1，型号名称选择WA2620E-AGN，并配置其序列号。
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 210235A42MB108000002
[AC-wlan-ap-ap1] map-configuration apcfg.txt
进入radio 1射频视图。
[AC-wlan-ap-ap1] radio 1
配置射频的工作信道为161。
[AC-wlan-ap-ap1-radio-1] channel 161
将无线服务模板service1绑定到AP的radio 1口。
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1]quit
(6)　配置Portal认证
配置Portal认证服务器地址为8.1.1.50，并指定服务器对应的URL。
[AC] portal server pt ip 8.1.1.50 key simple 123456 url http://8.1.1.50:8080/portal
配置Portal免认证规则1，用来放行AC上配置Portal认证服务的接口能够与Portal服务器通信。
[AC] portal free-rule 1 source interface bridge-aggregation1 destination any
配置AC通过WLAN获取Portal用户信息。
[AC] portal host-check wlan
配置RADIUS方案portal。
[AC] radius scheme portal
配置认证、计费和授权服务器的IP地址为8.1.1.50。
[AC-radius-portal] primary authentication 8.1.1.50
[AC-radius-portal] primary accounting 8.1.1.50
配置与认证、计费和授权服务器交互报文时的共享密钥为123456。
[AC-radius-portal] key authentication simple 123456
[AC-radius-portal] key accounting simple 123456
指定发送给RADIUS服务器的用户名不携带域名。
[AC-radius-portal] user-name-format without-domain
配置设备发送RADIUS报文使用的源IP地址为138.10.1.80。
[AC-radius-portal] nas-ip 138.10.1.80
[AC-radius-portal] quit
配置AAA认证域portal。
[AC] domain portal
设置ISP域的认证、授权和计费方法均为RADIUS。
[AC-isp-portal] authentication portal radius-scheme portal
[AC-isp-portal] accounting portal radius-scheme portal
[AC-isp-portal] authorization portal radius-scheme portal
[AC-isp-portal] quit
配置接口VLAN 30为Portal直接认证的接口。
[AC] interface vlan-interface 30
[AC-Vlan-interface30] portal server pt method direct
指定从接口接入的IPv4 Portal用户使用认证域为portal。
[AC-Vlan-interface30] portal domain portal
配置接口发送Portal报文使用的IPv4源地址为138.10.1.80。
[AC-Vlan-interface30] portal nas-ip 138.10.1.80
开启Portal本地转发功能。
[AC-Vlan-interface30] portal forwarding-mode local
[AC-Vlan-interface30] quit
配置AC与AP和Portal服务器通信的静态路由下一跳为Switch A的接口VLAN 10。
[AC] ip route-static 0.0.0.0 0 138.10.1.1
开启arp-snooping功能。
[AC] arp-snooping enable
开启learn-ipaddr功能

[AC] wlan client learn-ipaddr enable

3、配置SwitchB

配置GigabitEthernet1/0/1的类型为Trunk，允许所有VLAN通过。
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/1] quit
配置GigabitEthernet1/0/2接口属性，使能PoE为AP供电，类型为Trunk，允许所有VLAN通过。
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] poe enable
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan all

4、apcfg.txt配置文件

配置Portal服务器地址为8.1.1.50，并指定服务器对应的url。
system-view
portal server pt ip 8.1.1.50 key simple 123456 url http://8.1.1.50:8080/portal
配置Portal免认证规则1，用来放行AP上开启Portal认证服务的接口能够与Portal服务器通信。
portal free-rule 1 source interface GigabitEthernet 1/0/1 destination any
配置需求的Portal参数。
portal device-id beijing-ac-01
portal url-param include nas-id param-name vlan
portal url-param include user-mac des-encrypt param-name wlanusermac
portal url-param include nas-ip param-name wlanacip
portal url-param include ap-mac param-name wlanapmac
portal url-param include user-url param-name wlanfirsturl
portal url-param include user-ip param-name wlanuserip
portal url-param include ac-name param-name wlanacname
portal url-param include ssid
 portal host-check wlan
创建ACL 2000。
acl number 2000
创建rule,匹配所有源。
rule 0 permit
#进入接口VLAN 1视图
interface Vlan-interface1
#配置静态NAT，并将ACL 2000关联
nat outbound 2000
创建vlan 30。
vlan 30
创建VLAN 30对应接口，并进入接口VLAN 30视图
interface vlan 30
接口下指定Portal服务器并配置为直接认证方式。
 portal server pt method direct
接口下配置IP地址。
ip address 192.168.1.1 255.255.0.0
配置接口发送Portal报文使用的源地址为AC的地址。
 portal nas-ip 138.10.1.80
进入到AP的物理接口GigabitEthernet1/0/1。
interface GigabitEthernet 1/0/1
配置接口GigabitEthernet1/0/1类型为Trunk。
 port link-type trunk
配置接口GigabitEthernet1/0/1允许所有VLAN通过。
 port trunk permit vlan all

（1）AP注册需要预先配置AC的静态IP，或者由分支设备下发option 43属性。
（2）由AP作为各节点终端设备的业务网关，可以避免对其他设备繁琐的配置操作。
（3）仅V5 11n、11ac的AP支持NAT，V7 AP不支持NAT。