802.1X 分层AC **殷俊** 2018-10-30 发表

组网及说明

如所示,总部通过一台传统AC作为Central AC,分支采用融合AC作为Local AC,Local AC负责管理和 接入本地AP和无线客户端。用户的认证授权则由总部Central AC负责,数据流量由AP转发。 具体应用需求如下:

· AP通过DHCP Option43功能获取到Central AC地址,之后通过二次发现方式与Local AC建立 CAPWAP连接。

- · 使用iMC作为DOT1X服务器和AAA服务器对用户进行DOT1X认证。
- · AP和用户的地址池配置在Local AC上。



配置步骤

1.1.1 设置设备角色 (仅针对中端AC设备) (1) 设置设备角色为Central AC #普通AC, 配置Local AC模板设置角色为Central AC <AC> system-view [AC]wlan local-ac name localac1 model WX2540H #原设备为Local AC角色,去使能Local AC,配置Local AC模板切换角色为Central AC <AC> system-view [AC] [AC]undo wlan local-ac enable This operation will delete AC hierarchy settings for the local AC. Continue? [Y/ N]:y [AC]wlan local-ac name localac1 model WX2540H (2) 设置设备角色为Local AC #普通AC,使能Local AC功能设置角色为Local AC [AC]wlan local-ac enable #原设备为Central AC角色,删除所有Local AC模板,使能Local AC功能切换角色为Local AC [AC]undo wlan local-ac name localac1 [AC]wlan local-ac enable 1.1.2 编辑AP配置文件 #使用文本文档编辑AP的配置文件,将配置文件命名为map.txt,并将配置文件上传到AC存储介质上。 配置文件内容和格式如下: system-view interface GigabitEthernet1/0/1 port link-type trunk port trunk permit vlan all interface GigabitEthernet1/0/2 port link-type trunk port trunk permit vlan all 1.1.3 配置Central AC (1) 配置接口 #创建VLAN11及其接口,用来与Local AC建立管理通道。

<Central AC> system-view [Central AC] vlan 11 [Central AC-vlan11] quit [Central AC] interface vlan-interface 11 [Central AC-Vlan-interface11] ip address 11.1.1.3 16 [Central AC-Vlan-interface11] quit 配置Central AC管理的Local AC (2)# 创建名称为3510h-1的Local AC,并进入Local AC视图。 [Central AC] wlan local-ac name 3510h-1 model WX3510H #配置Local AC的序列号。 [Central AC-wlan-local-ac-3510h-1] serial-id 210235A1JNB166000078 [Central AC-wlan-local-ac-3510h-1] quit 配置无线客户端的DOT1X认证功能 (3)配置RADIUS方案 #创建RADIUS方案imc并进入其视图。 [Central AC] radius scheme imc # 设置主认证RADIUS服务器的IP地址8.1.1.231。 [Central AC-radius-imc] primary authentication 8.1.1.231 # 设置主计费RADIUS服务器的IP地址8.1.1.231。 [Central AC-radius-imc] primary accounting 8.1.1.231 # 设置系统与认证RADIUS服务器交互报文时的共享密钥为12345678。 [Central AC-radius-imc] key authentication simple 12345678 # 设置系统与计费RADIUS服务器交互报文时的共享密钥为12345678。 [Central AC-radius-imc] key accounting simple 12345678 #设置发送给RADIUS服务器的用户名不携带域名。 [Central AC-radius-imc] user-name-format without-domain #设置设备发送RADIUS报文时使用的源IP地址8.183.1.61。 [Central AC-radius-imc] nas-ip 8.183.1.61 [Central AC-radius-imc] quit 配置认证域 # 创建imc域并进入其视图。 [Central AC] domain imc #为DOT1X用户配置认证方案为RADIUS方案,方案名为imc。 [Central AC-isp-imc] authentication lan-access radius-scheme imc #为DOT1X用户配置授权方案为RADIUS方案,方案名为imc。 [Central AC-isp-imc] authorization lan-access radius-scheme imc #为DOT1X用户配置计费方案为RADIUS方案,方案名为imc。 [Central AC-isp-imc] accounting lan-access radius-scheme imc [Central AC-isp-imc] quit (4) 配置802.1X认证方式 #配置802.1X认证方式为EAP [Central AC]dot1x authentication-method eap

(5) 配置Dot1x服务模板#创建无线服务模板1。[Central AC]wlan service-template1

[Central AC -wlan-st-1]ssid qucf-dot1x #配置DOT1X认证点为Central AC,转发点为AP [Central AC -wlan-st-1]client-security authentication-location central-ac [Central AC -wlan-st-1]client forwarding-location ap

#配置用户认证方式为802.1X, ISP域为imc, AKM模式为802.1X, 加密套件为CCMP, 安全IE为RSN [Central AC -wlan-st-1]akm mode dot1x [Central AC -wlan-st-1]cipher-suite ccmp [Central AC -wlan-st-1]security-ie rsn [Central AC -wlan-st-1]client-security authentication-mode dot1x [Central AC -wlan-st-1]dot1x domain imc #使能服务模板 [Central AC -wlan-st-1]service-template enable (6) 配置AP模板 #创建手工AP,名称为ap1,配置序列号为210235A1SVC15C000028。 [Central AC] wlan ap ap1 model WA5620i-ACN [Central AC-wlan-ap-ap1] serial-id 210235A1SVC15C000028 #指定AP的配置文件。 [Central AC-wlan-ap-ap1] map-configuration cfa0:/map.txt #开启二次发现AC功能。 [Central AC-wlan-ap-ap1] control-address enable #手动指定Local AC的IP地址。 [Central AC-wlan-ap-ap1] control-address ip 11.1.1.104 #将无线服务模板1绑定到Radio 1接口。 [Central AC-wlan-ap-ap1] radio 1 [Central AC-wlan-ap-ap1-radio-1] radio enable [Central AC-wlan-ap-ap1-radio-1] service-template 1 vlan 20 [Central AC-wlan-ap-ap1-radio-1] quit 1.1.4 配置Local AC (1) 开启Local AC功能 #开启Local AC功能。 <Local AC> system-view [Local AC] wlan local-ac enable #指定Central AC的IP地址。 [Local AC] wlan central-ac ip 11.1.1.3 # 指定与Central AC建立管理通道的VLAN。 [Local AC] wlan local-ac capwap source-vlan 11 (2) 配置地址池 #开启DHCP服务。 [Local AC] dhcp enable #配置地址池,为AP分配IP地址。 [Local AC] dhcp server ip-pool ap [Local AC-dhcp-pool-ap] gateway-list 12.0.0.1 [Local AC-dhcp-pool-ap] network 12.0.0.0 mask 255.255.0.0 # 通过option43选项指定AC地址为Central AC地址。 [Local AC-dhcp-pool-ap] option 43 hex 80070000010b010101 [Local AC-dhcp-pool-ap] quit # 配置地址池,为客户端分配IP地址。 [Local AC] dhcp server ip-pool client [Local AC-dhcp-pool-ap] gateway-list 20.0.0.1 [Local AC-dhcp-pool-ap] network 20.0.0.0 mask 255.255.0.0 [Local AC-dhcp-pool-ap] quit (3) 配置接口 #创建VLAN11及其接口, Local AC通过此接口上线到Central AC。 [Local AC] vlan 11 [Local AC-vlan11] quit [Local AC] interface Vlan-interface11 [Local AC-Vlan-interface11] ip address 11.1.1.104 255.255.0.0 [Local AC-Vlan-interface11] quit #创建VLAN12及其接口,用于AP上线。 [Local AC] vlan 12 [Local AC-vlan12] quit [Local AC] interface Vlan-interface12 [Local AC-Vlan-interface12] ip address 12.0.0.1 255.255.0.0 [Local AC-Vlan-interface12] dhcp server apply ip-pool ap [Local AC-Vlan-interface12] quit # 创建VLAN20及其接口,用于无线客户端上线。 [Local AC] vlan 20 [Local AC-vlan20] quit [Local AC] interface Vlan-interface20 [Local AC-Vlan-interface20] ip address 20.0.0.1 255.255.0.0 [Local AC-Vlan-interface20] dhcp server apply ip-pool client [Local AC-Vlan-interface20] quit

验证配置:

在Central AC上可以查看到Local AC是R/M状态,说明Local AC已在Central AC上线。 [Central AC]display wlan local-ac name 3510h-1

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad C = Config, DC = DataCheck, R = RunAC name ACID State Model Serial ID 1 R/M WX3510H 210235A1JNB166000078 3510h-1 # 在Central AC上可以查看到AP是R/M状态,说明Local AC已经通过二次发现与Central AC建立管理 通道。 [Central AC]display wlan ap all Total number of APs: 1 Total number of connected APs: 1 Total number of connected manual APs: 1 Total number of connected auto APs: 0 Total number of connected common APs: 1 Total number of connected WTUs: 0 Total number of inside APs: 0 Maximum supported APs: 6144 Remaining APs: 6143 Total AP licenses: 128 Local AP licenses: 128 Server AP licenses: 0 Remaining Local AP licenses: 127 Sync AP licenses: 0 AP information

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad C = Config, DC = DataCheck, R = Run, M = Master, B = Backup

Local AC Information

AP name AP ID State Model Serial ID ap1 4 R/M WA562U-ACN 210235A1SVC15C000028 #在Central AC上可以查干到AP已经连接到Local AC。 [Central AC]display war ap-distribution all Central AC Slot 1 Total Number of APs: 0

Local AC 3510h-1 Total Number of APs: 1 AP name AP ID AP IP AC IP ap1 4 12.0.0.2 12.0 0.1 # 在Central AC上可以查看到无线客户端已经上线。 [Central AC]display wlan client Total number of clients: 1

MAC address User name AP name RID IP address VLAN e49a-dc71-a162 N/A ap1 1 20.0.0.2 20 #在Central AC上可以查看到用户已经DOT1X认证成功。 [Central AC] dis dot1x connection Total connections: 1 User MAC address : e49a-dc71-a162 AP name : ap1 : 1 : qucf-dot1x Radio ID SSID BSSID : 3891-d59a-7960 Username : qucf-1x BSSID Authentication domain : imc IPv4 address : 20.0.0.2 Authentication method : EAP Initial VLAN : 20 Authorization VLAN : 20 Authorization ACL number : 3000 Authorization user profile : N/A Termination action : Default Session timeout period : 86400 s Online from : 2018/10/22 11:31:18 : 0h 2m 12s Online duration

配置关键点

. 获取。

· Local AC上不能开启自动AP功能,对于需要在Central AC上统一管理的AP,也不要在Local AC上配置此AP模板。

· 高端AC仅支持Central AC角色,低端AC仅支持做Local AC角色,中端AC两种角色均支持且 两种角色互斥不能同时存在。中端AC通过配置命令切换角色,通过创建Local AC模板设置角色为Cent ral AC;通过使能Local AC设置角色为Local AC。注意角色切换后命令行由用户保证设备。