

某局点无线控制器Portal逃生功能异常问题处理经验案例

Portal 陈少华 2017-12-28 发表

在服务模板下开启了Portal逃生功能（portal fail-permit web-server）后终端可以直接上网，undo掉就回复正常。测试该类现象仅在某些楼栋，部分楼栋未出现该问题。

设备版本：

H3C WX5540H Version 7.1.064, Release 5215P01

iMC iMC PLAT 7.2 (E0403P10)

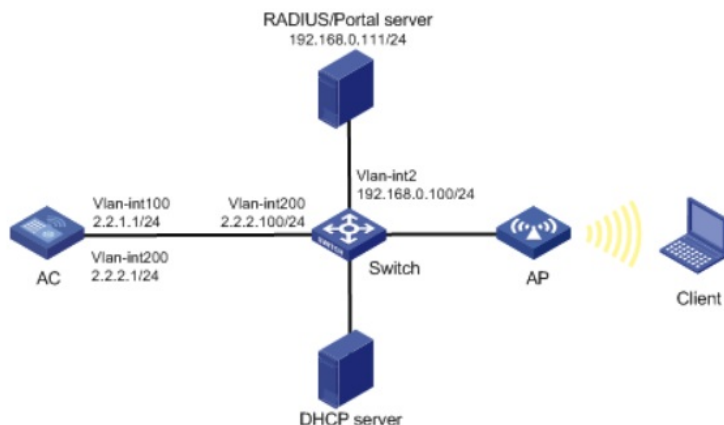
iMC EIA 7.2 (E0411P04)

组网：

AP和Client通过DHCP服务器获取IP地址，iMC同时作为Portal认证服务器、Portal Web服务器和RADIUS服务器，要求：

1. AC采用直接方式的Portal认证。
2. Client在通过Portal认证前，只能访问Portal Web服务器。Client通过Portal认证后，可以访问外部网络。
3. Client的数据流量直接由AP进行转发。
4. 用户可以在VLAN内的任何二层端口上访问网络资源，且移动接入端口时无须重复认证。
5. iMC服务器需要对用户授权信息进行动态修改或强制用户下线。
6. 为了使用户正常访问Portal Web服务器，配置Portal 免认证规则，放行访问Portal Web服务器的流量。

图1 本地转发模式下Portal直接认证组网图



1. 查看当前AC服务模板配置是否正确：

```
wlan service-template test
ssid JNU-test
vlan 511
client forwarding-location ap
portal enable method direct
portal domain jnu-guest
portal bas-ip 10.162.4.254
portal apply web-server jnu-guest
portal fail-permit web-server
service-template enable
web-server:
portal web-server jnu-guest
url http://192.168.11.34:8080/portal/
server-detect interval 60 trap
```

2. 查看iMC配置，无明显配置异常：

Portal服务器配置

基本信息

日志级别 *

Portal Server

报文请求超时时长(秒) * ⓘ

逃生心跳间隔时长(秒) * ⓘ

用户心跳间隔时长(分钟) * ⓘ

LB设备地址

Portal Web

请求报文超时时长(秒) * ⓘ

交互报文编码

校验终端用户请求报文

使用缓存

HTTP心跳界面展示方式

HTTPS心跳界面展示方式

Portal主页
https://192.168.11.34:8443/portal/

高级信息

修改设备信息

设备信息

设备名 *

版本 *

监听端口 *

认证重发次数 *

支持逃生心跳 *

密码 *

组网方式 *

设备描述

业务分组 *

IP地址 *

本端Challenge *

下连接失败数 *

支持用户心跳 *

确认密码 *

确定 取消

3. 继续分析Portal逃生实现原理，Portal逃生方案实现以下两大功能：

(1) 周期性探测Portal服务器

通过可配置的探测方法（在下面提到有两种探测方式）周期性探测Portal服务器，若Portal服务器N次（N可配）不可达则变成Down状态（逃生状态），取消网络的认证限制，允许Portal用户不需经过认证即可访问网络资源，并发送状态改变的Trap信息和日志。当探测到服务器可达时，恢复服务器状态为Up状态（认证状态），并重新开启网络认证限制，不允许未认证的用户访问网络，并发送状态恢复的日志和Trap。

(2) 设备和Portal服务器同步用户信息

Portal服务器定时将自己的在线用户信息周期性地通过用户信息同步报文发送给接入设备。如果同步报文中包含了设备上不存在的用户信息，则接入设备会将这些用户信息返回给Portal服务器，由Portal服务器将其强制下线。如果某用户连续N个周期（N可配）都未在从Portal服务器发送过来的同步报文中出现，则接入设备会将该用户强制下线。

当前应用场景下采取的是第一种周期性探测方案，即当Portal服务器不可达或者Portal服务不能正常工作时，设备可以临时放开对用户访问网络的认证限制，不中断或停止用户的正常网络访问，当Portal服务器恢复后，设备再恢复为正常认证状态，减少了服务器故障给用户业务带来的影响。

(3) 查看Portal Web-server，判断服务器探针是否正常

通过开启Portal Web 服务器的可达性探测功能之后，接入设备采用模拟用户进行 Web 访问的过程来实施探测：

接入设备主动向Portal Web 服务器发起 TCP 连接，如果连接可以建立，则认为此次探测成功且服务器可达，否则认为此次探测失败。当AC探测不通Web服务器不通时，则Portal Web-server状态变成Down，所有终端放通免认证。

[H3C]display portal web-server

Portal Web server: newpor

Type : CMCC

URL : <http://192.168.0.111:8080/portal>

URL parameters : ssid=ssid

VPN instance : Not configured

Server detection : Interval: 30 s Attempts: 3 Action: trap

IPv4 status : up

IPv6 status : N/A

Captive-bypass : Disabled

If-match : Not configured

在终端放通免认证后，AC设备侧查看portal Web-server状态为UP状态，无明显异常。

(4) 分析Portal服务器探测方式

接入设备探测Portal服务器状态的具体实现方式有以下两种：

探测HTTP连接：接入设备定期向Portal服务器的HTTP服务端口发起TCP连接。若连接成功建立则表示此服务器的HTTP服务已开启，就认为一次探测成功且服务器可达（状态为Up）；若连接失败则认为一次探测失败。

探测Portal心跳报文：支持Portal逃生心跳功能的Portal服务器（目前仅iMC支持）会定期向接入设备发送Portal心跳报文，设备通过检测此报文来判断服务器的可达状态：若设备在指定的周期内收到Portal心跳报文或者其它认证报文，且验证其正确，则认为此次探测成功且服务器可达（状态为Up），否则

认为此次探测失败。

在实际应用中，支持只采用其中一种探测方式或同时采用两种探测方式。如果同时采用了两种探测方式，则只要其中任何一种探测方式结果表明服务器不可达，即认为服务器不可达。而在服务器不可达状态下，只有采用两种探测方式的探测都成功后才能认为服务器恢复为可达状态。

继续分析当前组网形态，AP采取本地转发模式，数据直接由本地上行转发，不经过AC绕行。接入设备和Portal服务器链接状态由AP与Portal服务器侧维系。需测试AP侧与Portal服务器连接状态。

(5) 测试AP与Portal Web-server连通性

通过在两栋楼栋间远程到AP分别ping包Portal Web-server检测发现，Portal逃生功能正常楼栋，AP与Portal Web-server连通性良好，正常ping包。Portal逃生功能异常楼栋，AP与Portal Web-server ping包无法互通。即此，怀疑为AP侧与Portal Web-server连通性异常，导致AP与Portal服务器不可达，设备临时放开对用户访问网络的认证限制，用户可直接上网。

(6) 排查AP到Portal Web-server连通性问题

通过排查链路侧问题，发现防火墙未放通该楼栋vlan地址段，导致AP客户链到Portal Web-server数据不通，属于配置错误，修改后再测试，功能正常。

排查AP到Portal Web-server连通性问题，通过排查发现防火墙未放通该楼栋vlan地址段，导致AP客户链到Portal Web-server数据不通，属于配置错误，修改后再测试，功能正常。