H3C WX 系列本地 Portal Server 典型配置举例

关键词：Local-Server，本地 Portal Server

摘　要：本文介绍了用 H3C 公司 WX 系列 AC 部署本地 Portal Server 解决方案时必需的配置。

缩略语：

缩略语	英文全名	中文解释
AC	Access Control	无线控制器
AP	Access Point	无线接入点
ESS	Extended Service Set	扩展服务集
WLAN	Wireless Local Area Network	无线局域网
SSID	Service Set Identifier	服务集识别码
AAA	Authentication, Authorization and Accounting	认证、授权和计费
iMC	Intelligent Management Center	智能管理中心
RADIUS	Remote Authentication Dial-In User Service	远程认证拨号用户服务

目　录

1 特性简介 1
1.1 特性介绍 1
1.2 特性优点 1
2 应用场合 1
3 注意事项 1
4 配置举例 2
4.1 组网需求 2
4.2 配置思路 2
4.3 使用版本 2
4.4 配置步骤 3
4.5 注意事项 12
5 相关资料 12
5.1 相关协议和标准 12
5.2 其它相关资料 12

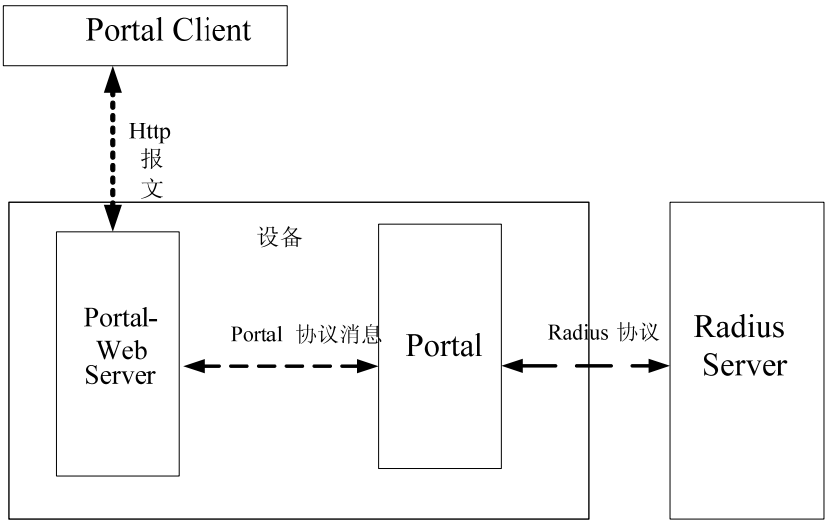
1 特性简介

1.1 特性介绍

Portal 基本功能的实现需要 4 个元素：Portal Server，RADIUS 服务器，支持 Portal 协议的接入设备，Portal 客户端。其中 Portal Server 的作用是，接受 Portal 客户端认证请求的服务器端系统，提供基于 Web 认证的界面，与接入设备交互认证客户端的认证信息。

设备内嵌 Portal-Web Server 能够解析客户端发来的 http 上线认证、下线，形成认证、下线请求给 Portal 模块，然后根据返回的结果，推出对应的页面给客户端。这样设备就支持 web 用户直接登录而不需要额外的部署 Portal Server。从而大大加强了 Portal 功能的通用性，如图 1-1 所示。

图1 设备内嵌 Portal-Web Server 的框图



从图 1-1 可以看出：Portal-Web Server 和 Portal 客户端之间是 http 协议报文，发送用户的登录请求、下线请求；设备 Portal-Web Server 解析 http 请求，封装成 Portal-Web Server 模块与 Portal 模块之间的消息，传递给 Portal 模块；Portal 接收到消息后，触发相应的动作，向 Radius Server 发送认证、授权和计费报文。

1.2 特性优点

本特性丰富了 Portal 特性，简化了 Portal 的部署，不需要额外部署 Portal Server，大大加强了 Portal 模块的通用性。

2 应用场合

当部署 Portal 业务而不想使用单独的 Portal Server（如 iMC）的时候，可以使用本特性。

3 注意事项

(1) 接入设备上服务器端口配置正确。

(2) 相关 AAA 配置正确。

4 配置举例

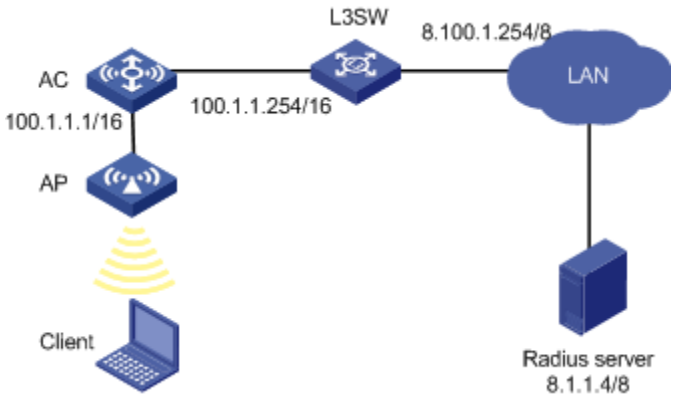
4.1 组网需求

说明

本配置举例中的 AC 使用的是 WX3000 系列有线无线一体化交换机设备，IP 地址为 100.1.1.1/16。Client 和 AP 通过 DHCP 服务器获取 IP 地址。

Radius server 的 IP 地址为 8.1.1.4/8。三层交换机 L3SW 的两个接口地址分别是 100.1.1.254/16 和 8.100.1.254/8。

图2 本地 Portal Server 组网图



4.2 配置思路

- 配置 Portal 功能。
- 配置 Radius 服务器（说明：如果在远程做认证则在 Radius 服务器上配置用户名和服务；在本地进行认证，则在本地创建用户）。

4.3 使用版本

```
<AC> display version
H3C Comware Platform Software
Comware Software, Version 5.20, Beta 3105
Copyright (c) 2004-2008 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
```

```
H3C WX3024 uptime is 0 week, 0 day, 9 hours, 43 minutes

H3C WX3024 with 1 RMI XLS 208 750MHz Processor
256M bytes DDR2
56M bytes Flash Memory
Config Register points to FLASH

Hardware Version is Ver.A
CPLD Version is 002
Basic Bootrom Version is 1.05
Extend Bootrom Version is 1.05
[Slot 0]WX3024LSW Hardware Version is NA
[Slot 1]WX3024RPU Hardware Version is Ver.A

[AC]
```

4.4 配置步骤

1. 配置信息：

```
<AC> display current-configuration
#
 version 5.20, Beta 3105
#
 sysname AC
#
 domain default enable iMC
#
 portal server loc10 ip 100.10.1.1 url http://100.10.1.1
 portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
 portal local-server http
#
vlan 1
#
vlan 10
#
vlan 100
#
radius scheme iMC
 server-type extended
 primary authentication 8.1.1.4
 primary accounting 8.1.1.4
 key authentication admin
 key accounting admin
 user-name-format without-domain
radius scheme system
 primary authentication 127.0.0.1
 primary accounting 127.0.0.1
 key authentication admin
```

```
 key accounting admin
 accounting-on enable
#
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
#
user-group system
#
wlan rrm
 dot11a mandatory-rate 6 12 18 24
 dot11a supported-rate 9 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 3 clear
 ssid clear
 bind WLAN-ESS 3
 service-template enable
#
interface NULL0
#
interface LoopBack0
#
interface Vlan-interface1
 ip address 100.1.1.1 255.255.0.0
#
interface Vlan-interface10
 ip address 100.10.1.1 255.255.0.0
 portal server loc10 method direct
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 1 10 100 tagged
#
interface WLAN-ESS3
```

```
 port access vlan 10
#
wlan ap 12 model WA2100
 serial-id 210235A22W0073000002
 radio 1
  service-template 3
  radio enable
#
 ip route-static 8.1.0.0 255.255.0.0 100.1.1.254
#
 snmp-agent
 snmp-agent local-engineid 800063A203000FE2129876
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
#
 load xml-configuration
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
<AC>
```

2. 主要配置步骤

(1) 配置认证策略。

创建 RADIUS 方案 iMC 并进入其视图。

```
[AC] radius scheme iMC
```

将 RADIUS 方案 iMC 的 RADIUS 服务器类型设置为 extended。

```
[AC-radius-iMC] server-type extended
```

设置主认证 RADIUS 服务器的 IP 地址 8.1.1.4。

```
[AC-radius-iMC] primary authentication 8.1.1.4
```

设置主计费 RADIUS 服务器的 IP 地址 8.1.1.4。

```
[AC-radius-iMC] primary accounting 8.1.1.4
```

设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 admin。

```
[AC-radius-iMC] key authentication admin
```

设置系统与计费 RADIUS 服务器交互报文时的共享密钥为 admin。

```
[AC-radius-iMC] key accounting admin
```

指定发送给 RADIUS 方案 iMC 中 RADIUS 服务器的用户名不得携带域名。

```
[AC-radius-iMC] user-name-format without-domain
[AC-radius-iMC] quit
```

(2) 配置认证域。

创建 iMC 域并进入其视图。

```
[AC] domain iMC
```
为 Portal 用户配置认证方案为 RADIUS 方案，方案名为 iMC。
```
[AC-isp-iMC] authentication portal radius-scheme iMC
```
为 Portal 用户配置授权方案为 RADIUS 方案，方案名为 iMC。
```
[AC-isp-iMC] authorization portal radius-scheme iMC
```
为 Portal 用户配置计费方案为 RADIUS 方案，方案名为 iMC。
```
[AC-isp-iMC] accounting portal radius-scheme iMC
[AC-isp-iMC] quit
```
(3) 把配置的认证域 IMC 设置为系统缺省域。
```
[AC] domain default enable iMC
```
(4) 配置无线服务模板。

创建 clear 类型的服务模板 3。
```
[AC] wlan service-template 3 clear
```
设置当前服务模板的 SSID（服务模板的标识）为 clear。
```
[AC-wlan-st-3] ssid clear
```
将 WLAN-ESS3 接口绑定到服务模板 3。
```
[AC-wlan-st-3]bind WLAN-ESS 3
```
使能服务模板。
```
[AC-wlan-st-3]service-template enable
[AC-wlan-st-3]quit
```
(5) 配置无线口 WLAN-ESS 3，将无线口添加到起 Portal 的 VLAN10。
```
[AC] interface WLAN-ESS 3
[AC-WLAN-ESS3] port access vlan 10
[AC-WLAN-ESS3] quit
```
(6) 在 AC 下绑定无线服务模板。

注意：AP 的配置需要根据具体的 AP 型号和 AP 序列号进行配置。

创建 AP 管理模板，其名称为 12，型号名称这里选择 WA2100。
```
[AC] wlan ap 12 model WA2100
```
设置 AP 的序列号为 210235A22W0073000002。
```
[AC-wlan-ap-12] serial-id 210235A22W0073000002
```
进入 radio 1 射频视图。
```
[AC-wlan-ap-12] radio 1
```
将在 AC 上配置的 clear 类型的服务模板 3 与射频 1 进行关联。
```
[AC-wlan-ap-12-radio-1] service-template 3
```
使能 AP 的 radio 1。
```
[AC-wlan-ap-12-radio-1] radio enable
[AC-wlan-ap-12-radio-1] quit
```
(7) 配置 Portal Server 和免认证规则。

配置 Portal 服务器 loc10 的 IP 地址为 100.10.1.1、HTTP 重定向的 URL 为 http://100.10.1.1。
```
[AC] portal server loc10 ip 100.10.1.1 url http://100.10.1.1
```
配置 Portal 免认证规则 0，符合源接口为 GigabitEthernet1/0/1 的任意报文不会触发 Portal 认证。

```
[AC] portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
```

配置本地 Portal 服务器支持 HTTP 协议方式。

```
[AC] portal local-server http
```

进入 VLAN 接口视图 10。

```
[AC] interface Vlan-interface 10
```

配置接口 IP 地址为 100.10.1.1 16。

```
[AC-Vlan-interface10] ip address 100.10.1.1 16
```

在接口 Vlan-interface10 上使能 Portal。指定 Portal 服务器为 loc10，并配置为直接认证方式。

```
[AC-Vlan-interface10] portal server loc10 method direct
[AC-Vlan-interface10] quit
```

对 free-rule 0 的说明补充：不配置该免认证规则时，从 GigabitEthernet1/0/1 进来的报文也被丢弃，用户通过认证后也 ping 不通外网（网关），加上该规则的目的就是让放开从该口进来的报文。

(8) 配置缺省路由

```
[AC]ip route-static 8.1.0.0 255.255.0.0 100.1.1.254
```

3. iMC配置

在 iMC 上配置接入设备（iMC 版本：3.20-R2606）如下：

(1) 在 iMC 上增加设备：

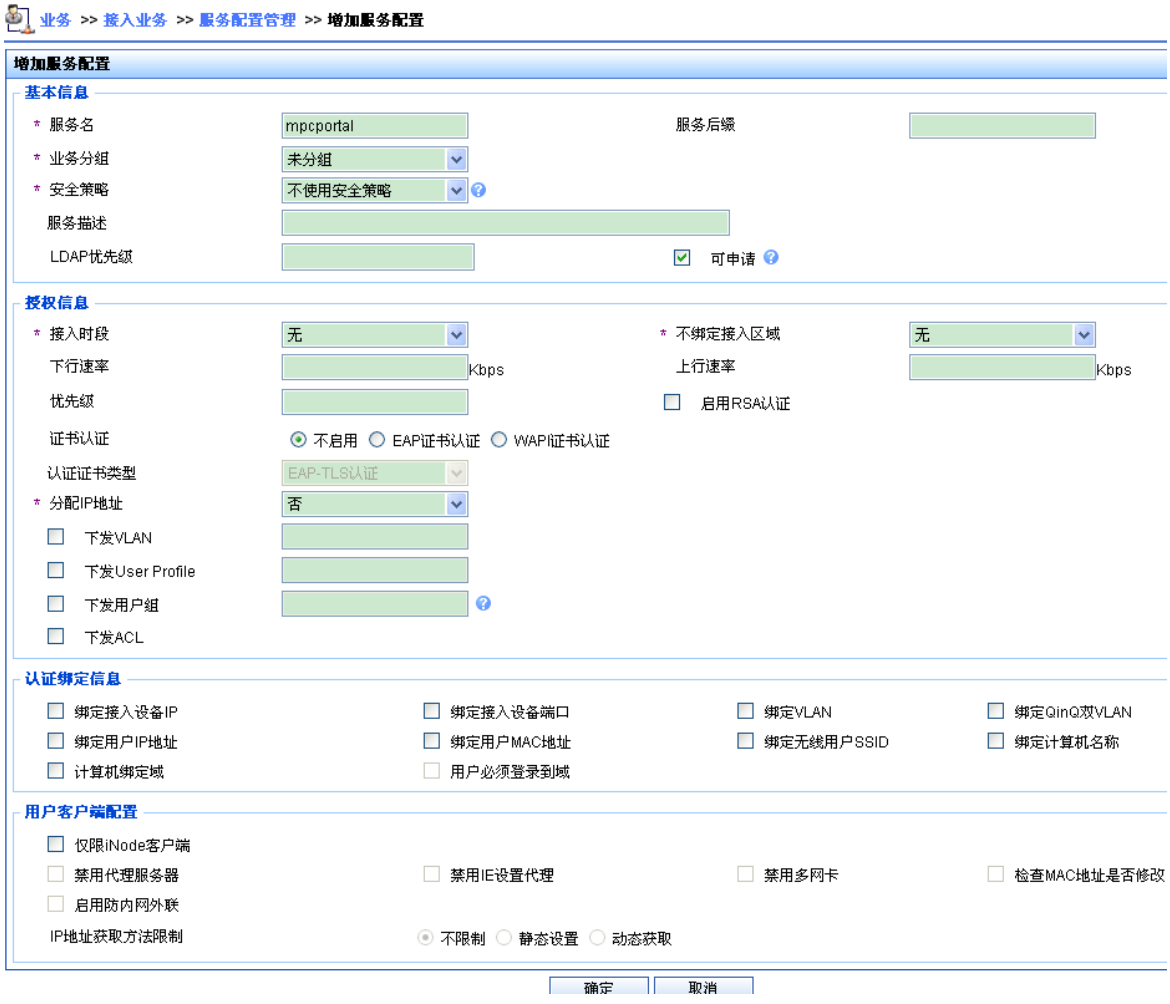
在 iMC“资源>资源管理”中单击“增加设备”，在“增加设备”页面中按下图所示配置参数：

(2) 配置接入设备

在导航栏中选择“业务->接入业务->接入设备配置”，点击<增加>按钮。在“增加接入设备”页面如下图所示配置参数：

(3) 配置服务策略：

在 iMC“业务>接入业务”中选择“服务配置管理”，在“服务配置管理”页面中单击<增加>按钮，在“增加服务配置”页面按下图所示配置参数：



(4) 配置帐号用户：

在 iMC “用户>所有接入用户>未分组”页面中，点击<增加>按钮，增加账号和用户，如下图所示：

添加账号名和密码，同时勾选在步骤（3）中创建的服务策略 mpcportal，然后点击<确定>按钮完成配置。Portal 用户登陆时，在 web 页面上输入账号名和密码就可以登录，如下图所示：

4. Portal认证页面定制配置（可选）

(1) 主索引页面文件命名

用户定制的主索引页面文件名不能自定义，必须使用 表 1 中所列的固定文件名。主索引页面文件之外的其他文件名可由用户自定义，但需注意文件名和文件目录名中不能含有中文且不区分大小写。

表1 认证页面文件名

主索引页面	文件名
登录页面	logon.htm
登录成功页面	logonSuccess.htm
登录失败页面	logonFail.htm
在线页面 用于提示用户已经在线	online.htm
系统忙页面 用于提示系统忙或者该用户正在登录过程中	busy.htm
下线成功页面	logoffSuccess.htm

(2) 认证页面的表单编辑原则

认证页面中表单（Form）的编辑必须符合以下原则：

- 认证页面可以含有多个Form，但是必须有且只有一个Form的action=logon.cgi，否则无法将用户信息送到本地 Portal 服务器。
- 用户名属性固定为“PtUser”，密码属性固定为”PtPwd”。
- 需要有用于标记用户登录还是下线的属性“PtButton”，取值为“Logon”表示登录，取值为“Logoff”表示下线。
- 登录 Post 请求必须包含“PtUser”，“PtPwd”和“PtButton”三个属性。
- 下线 Post 请求必须包含“PtButton”这个属性。

logon.htm 认证页面脚本内容的部分示例：

```
<form action=logon.cgi method = post >
<p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px" maxlength
=64>
<p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px" maxlength
=32>
<p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;">
</form>
```

online.htm 页面脚本内容的部分示例：

```
<form action=logon.cgi method = post >
<p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">
</form>
```

(3) 认证页面文件压缩及保存

- 完成所有认证页面的编辑之后，必须按照标准 Zip 格式将其压缩到一个 Zip 文件中，该 Zip 文件的文件名只能包含字母、数字和下划线。
- 压缩生成的 Zip 文件可以通过 FTP 或 TFTP 的方式上传至设备，且必须保存在设备根目录下的 portal 目录下。

Zip 文件保存目录示例：

```
<Sysname> dir
Directory of flash:/portal/
   0     -rw-      1405  Feb 28 2008 15:53:31   ssid2.zip
   1     -rw-      1405  Feb 28 2008 15:53:20   ssid1.zip
   2     -rw-      1405  Feb 28 2008 15:53:39   ssid3.zip
   3     -rw-      1405  Feb 28 2008 15:53:44   ssid4.zip
2540 KB total (1319 KB free)
```

说明

认证页面在文件大小和内容上需要有如下限制：每套页面（包括主索引页面文件及其页面元素）压缩后的 Zip 文件大小不能超过 500K 字节；每个单独页面（包括单个主索引页面文件及其页面元素）压缩前的文件大小不能超过 50K 字节；页面元素只能包含 HTML、JS、CSS 和图片之类的静态内容。

(4) 配置客户端 SSID 与定制的认证页面文件的绑定

最后，在 AC 上需要配置客户端 SSID 与定制的认证页面文件的绑定（该配置可选，如果没有配置则推出系统缺省的认证页面）。要绑定页面到名为 clear 的 SSID 上，对应的认证页面文件名为 ssid1.zip，且已保存在设备的 flash:/portal/目录下。

```
[AC] portal local-server bind ssid clear file ssid1.zip
```

5. 验证结果

(1) 使用 display portal user all 或者 display connection 查看 Portal 用户，有 Portal 用户在线。

```
<AC> display portal user all
 Index:99
 State:ONLINE
 SubState:NONE
 ACL:NONE
 MAC              IP               Vlan     Interface
 0017-9a00-7cb8   100.10.0.57      10       Vlan-interface10
 Total 1 user(s) matched, 1 listed.
<AC>
<AC> display connection
Index=103 ,Username=mpcportal@h3c
MAC=0017-9a00-7cb8   ,IP=100.10.0.57
 Total 1 connection(s) matched.
<AC>
<AC> display connection  ucibindex 103
Index=103 , Username=mpcportal@h3c
MAC=0017-9a00-7cb8
IP=100.10.0.57
Access=PORTAL  ,AuthMethod=PAP
Port Type=Wireless-802.11,Port Name=N/A
Initial VLAN=10, Authorization VLAN=N/A
```

```
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2008-11-06 10:54:51 ,Current=2008-11-06 10:54:59 ,Online=00h00m08s
 Total 1 connection matched.
<AC>
```

(2) 在 iMC 上查看用户在线。

在 iMC 中选择“用户>接入用户视图>所有在线用户>未分组”查看上线用户，如下图所示：

4.5 注意事项

无。

5 相关资料

5.1 相关协议和标准

无

5.2 其它相关资料

- 《H3C WX 系列无线控制产品 配置指导》“安全配置指导”中的“端口安全配置”、“AAA 配置”、“Portal 配置”。
- 《H3C WX 系列无线控制产品 命令参考》“安全命令参考”中的“端口安全命令”、“AAA 命令”、“Portal 命令”。
- 《H3C WX 系列无线控制产品 配置指导》“WLAN 配置指导”中的“WLAN 服务配置”、“WLAN 安全配置”。
- 《H3C WX 系列无线控制产品 命令参考》“WLAN 命令参考”中的“WLAN 服务命令”、“WLAN 安全命令”。