


```

[AC]#pki-domain-do|certificates ee
[AC]#pki-domain-do|certificates request ee
[AC]#pki-domain-do|certificates request ee ee
[AC]#pki-domain-do|cert check
[AC]#pki-domain-do|cert check ee
[AC]#pki-domain-do|cert check disable
[AC]#pki-domain-do|cert check ee
[AC]#pki-domain-do|cert check ee
[AC]#pki-domain-do|cert check ee
Warning: Confirm to destroy these keys? [Y/N]:
[AC]#pki import-certificates ca-domain do der filename certtem.cer
The trusted CA's fingerprint is:
  EE Fingerprint:0104 8AD7 57E1 51F7 6D2E 5D74 5D2E 5D4A
  0104 Fingerprint:0104 8AD7 57E1 51F7 6D2E 5D74 5D2E 5D4A
Is the above print correct?[Y/N]:
May 22 15:06:02:007 2009 H3C PE1/4/Write_CA_Root_Cert:CA root certificate of the domain do is trusted.....
Import CA certificate successfully.
May 22 15:06:02:151 2009 H3C PE1/4/Update_CA_Cert:Update CA certificates of the Domain do successfully.
[AC]
May 22 15:06:02:101 2009 H3C PE1/4/Import_CA_Cert:Import CA certificates of the domain do successfully.
[AC]
[AC]
[AC]
[AC]
[AC]#pki import-certificates ipsec-domain do der filename certipsec.cer
Please input challenge password:
May 22 15:06:02:000 2009 H3C PE1/4/Write_CA_Ipsec_Cert:CA ipsec certificate of the domain do successfully.....
Import ipsec certificate successfully.
May 22 15:06:02:094 2009 H3C PE1/4/Update_CA_Cert:Import CA certificates of the domain do successfully.
[AC]
May 22 15:06:02:000 2009 H3C PE1/4/Write_CA_Ipsec_Cert:CA ipsec certificate of the domain do successfully.....
Import ipsec certificate successfully.
[AC]

```

配置SSL服务策略

```

[AC]ssl server-policy 1
[AC-ssl-server-policy-1]pki-domain do
[AC-ssl-server-policy-1]handshake timeout 180
[AC-ssl-server-policy-1]close-mode wait
[AC-ssl-server-policy-1]session cachesize 1000

```

应用SSL服务策略、开启HTTPS服务

```

[AC]ip https ssl-server-policy 1
[AC]ip https enable

```

配置PKI实体和域

```

[AC]pki entity en
[AC-pki-entity-en]common-name portal
[AC-pki-entity-en]organization portal_server
[AC]pki domain do
[AC-pki-domain-do]certificate request entity en
[AC-pki-domain-do]crl check disable

```

配置认证策略

```

[AC]radius scheme cams
[AC-radius-cams]server-type extended
[AC-radius-cams]primary authentication 192.168.1.10
[AC-radius-cams]primary accounting 192.168.1.10
[AC-radius-cams]key authentication h3c
[AC-radius-cams]key accounting h3c
[AC-radius-cams]nas-ip 192.168.1.254

```

配置认证域

```

[AC]domain cams
[AC-isp-cams]authentication portal radius-scheme cams
[AC-isp-cams]authorization portal radius-scheme cams
[AC-isp-cams]accounting portal radius-scheme cams

```

配置无线服务模板

```

[AC]wlan service-template 2 clear
[AC-wlan-st-2]ssid lopo
[AC-wlan-st-2]bind WLAN-ESS 2
[AC-wlan-st-2]service-template enable

```

配置无线口，将无线口添加到起Portal的vlan

```

[AC]interface WLAN-BSS 2
[AC-WLAN-BSS2] port access vlan 2

```

在AC下绑定无线服务模板

```

[AC-wlan-ap-ap_001]wlan ap ap_001 model WA2220E-AG
[AC-wlan-ap-ap_001]serial-id 210235A22W0073000002
[AC-wlan-ap-ap_001]radio 2
[AC-wlan-ap-ap_001-radio-2]service-template 2
[AC-wlan-ap-ap_001-radio-2]radio enable

```

配置Portal Server和免认证规则

```

[AC]portal server local ip 192.168.1.254 url https://192.168.1.254/portal
[AC]portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
[AC]portal local-server https server-policy 1
[AC]interface Vlan-interface 2
[AC-Vlan-interface1]ip address 192.168.2.254 24
[AC-Vlan-interface1]portal server local method direct

```

四、WX3024交换机的典型配置

```
#
version 5.20, Beta 3105P01
#
sysname AC
#
domain default enable system
#
telnet server enable
#
port-security enable
#
portal server local ip 192.168.1.254 url https://192.168.1.254/portal
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
portal local-server https server-policy 1
#
oap management-ip 192.168.0.101 slot 0
#
vlan 1
#
vlan 2
#
radius scheme cams
server-type extended
primary authentication 192.168.1.10
primary accounting 192.168.1.10
key authentication h3c
key accounting h3c
nas-ip 192.168.1.254
#
domain cams
authentication portal radius-scheme cams
authorization portal radius-scheme cams
accounting portal radius-scheme cams
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
#
pki entity en
common-name portal
organization portal_server
#
pki domain do
certificate request entity en
crl check disable
#
dhcp server ip-pool vlan1
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.254
#
dhcp server ip-pool vlan2
network 192.168.2.0 mask 255.255.255.0
gateway-list 192.168.2.254
#
user-group system
#
local-user admin
password simple admin
```

```
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
#
wlan service-template 2 clear
ssid H3C-local-portal
bind WLAN-ESS 2
service-template enable
#
ssl server-policy 1
pki-domain do
handshake timeout 7200
close-mode wait
session cachesize 1000
#
interface NULL0
#
interface Vlan-interface1
ip address 192.168.1.254 255.255.255.0
#
interface Vlan-interface2
ip address 192.168.2.254 255.255.255.0
portal server local method direct
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
#
interface WLAN-ESS2
port access vlan 2
#
wlan ap ap_001 model WA2220E-AG
serial-id 210235A29F0081000109
radio 1
radio 2
service-template 2
radio enable
#
dhcp enable
#
ip https ssl-server-policy 1
ip https enable
#
load xml-configuration
#
user-interface aux 0
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
#
return
```

五、CAMS配置:

1、增加服务配置

服务管理 >> 服务配置 >> 查询服务

查询服务

基本信息			
服务名	cans (可申请)	服务后缀	cans
服务描述			
计费策略	不计费		
安全策略	不使用安全策略		
授权信息			
接入时段	不限	不绑定接入区域	无
下行速率	缺省值	上行速率	缺省值
优先级	缺省值		
<input type="checkbox"/> 动态IP分配	分配IP地址方式		
<input type="checkbox"/> 下发用户组 (SSL VPN专用):			
<input type="checkbox"/> 访问权限控制 (外部组、内部组)		外部组:	内部组:
认证绑定			
<input type="checkbox"/> 绑定接入设备IP	<input type="checkbox"/> 绑定接入设备端口	<input type="checkbox"/> 绑定VLAN	<input type="checkbox"/> 绑定用户IP地址
<input type="checkbox"/> 绑定用户MAC地址	<input type="checkbox"/> 绑定无线用户SSID	<input type="checkbox"/> 绑定计算机名称	
认证客户端配置			
<input type="checkbox"/> 校验CANS配置客户端			
<input type="checkbox"/> 禁用代理服务器	<input type="checkbox"/> 禁用IP设置代理	<input type="checkbox"/> 禁用多网卡	<input type="checkbox"/> 检查MAC地址是否修改
IP地址获取方法限制	不限		

[返回](#)

2. 增加用户帐号

用户管理 >> 帐号用户 >> 帐号维护

修改 | 出帐 | 缴费 | 暂停 | 黑名单 | 更改付费类型 | 强制下线 | 在线删除 | 时间补偿 | 销户

帐号信息 | 上网明细 | 用户帐单 | 缴费记录 | 认证失败日志 | 安全日志

帐号: cans

帐号用户信息

[打印](#)

帐号名	cans	帐号类型	预付费帐号
帐号状态	正常	帐号余额	0.00 元
用户姓名	cans	证件号码	
启用密码控制策略	否	下次登录须修改密码	否
联系方式		Email地址	
创建时间	2008-10-16	帐号失效时间	不限
设备IP地址		端口号	
VLAN ID		无线用户SSID	
是否绑定多IP、MAC地址	否	计算机名称	
用户IP地址		网卡MAC地址	
在线数量限制	10	最大闲置时长	不限
在线状态	不在线	修改密码/充值	不限
登录提示信息			

已申请的服务信息:

服务名	服务描述	计费策略	服务后缀	详细信息
cans		不计费	cans	查询

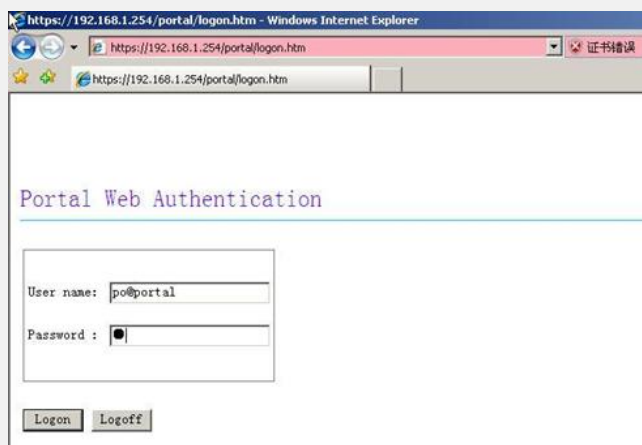
六、验证结果

1. RADIUS客户端的相关配置

在STA上打开IE，输入IP地址(在有DNS的情况下可直接输入网址)，弹出警报对话框，选择“继续浏览此网站”。



切换到HTTPS的认证页面，输入帐号，完成认证。



七、Q&A

WX3024设备上没有时钟芯片，设备重启后造成设置的时间丢失，导致导入的证书无法正常使用，因此需要重新导入。

重新导入证书的方法：

申请的根证书重命名为certnew.cer使用命令直接导入；

申请的服务器验证证书重命名为server_ssl.ptx，但需要删除原有证书再导入，删除原证书命令：

```
public-key local destroy rsa
```

```
(Y/N)y
```