Huawei Technologies Co.,Ltd.

华为证券轻型营业部解决方案 V100R001C00 配置指南

Zhouxiaowei 00200345

2013/9/30

商标声明

 和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。
由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司
地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129
网址： http://enterprise.huawei.com
客户服务邮箱： support_e@huawei.com
客户服务电话： 400-822-9999

前言

概述

本文档介绍了华为证券轻型营业部解决方案V100R001C00的组网配置操作，包括网络规划建议、基础网络配置、接入侧配置、WIFI配置、上网行为管理、统一管理、桌面云、离柜开户、数据中心网络接入等。

读者对象

本文档主要适用于以下工程师：

- 渠道商网规工程师
- 渠道商现场调试工程师
- 华为技术支持工程师

格式约定

格式	意义
粗体	注意事项或关键点
灰色底纹	表示设备的配置步骤的命令实例
//	备注或解释性质的文字
说明	以本标志开始的文本是正文的附加信息，是对正文的补充或强调

文档版本 01 （2013-11-30）

第一次正式发布。

目录

1 开局指引

关于本章

介绍本指导书的使用范围，以及各子解决方案的开局流程和准备工作要求。

1.1 适用范围

本节主要介绍本指导书适用范围。

1.2 开局流程

本节主要介绍开局流程和本指导书重点描述内容。

1.3 准备工作

本节主要介绍进行配置调试前需要做哪些准备工作。

1.1 适用范围

华为证券轻型营业部解决方案包括以下4个子方案：

- 证券一体机解决方案
- 离柜开户解决方案
- 桌面云解决方案
- 接入中心解决方案

针对不同类型轻型营业部，华为证券轻型营业部解决方案提出相应整体ICT解决方案。

说明：

本指导书未能满足您配置指导时请通过下面途径获寻帮助：

1） 资料链接：华为企业BG产品文档下载链接

2） **中国区维护热线：**400-822-9999（7*24小时）；**服务邮箱:** support_e@huawei.com。

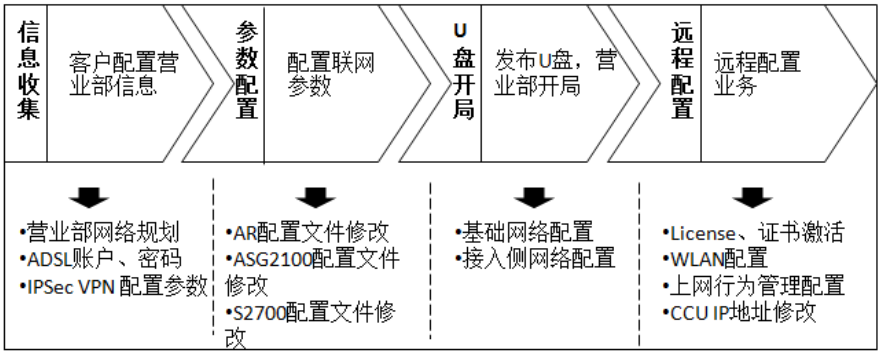
3） 联系华为负责此项目销售人员。

1.2 开局流程

- 证券一体机

通常交付流程是：交付前与客户交流获取营业部配置信息—>根据营业部配置修改U盘开局模板—>通过 U盘开局完成初步网络配置—>通过远程配置完成营业部剩余配置。

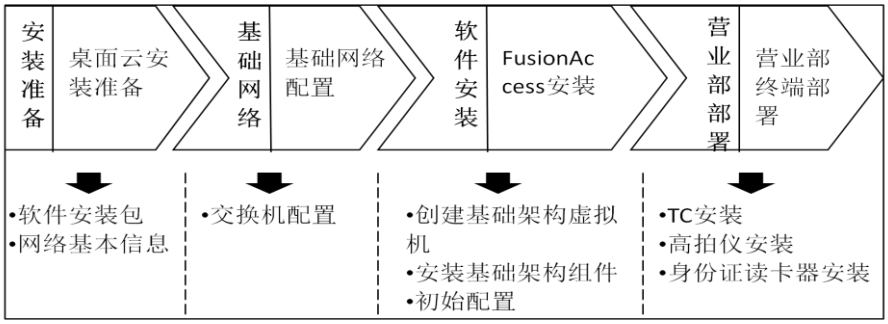
华为证券一体机解决方案开局流程如下：



- 桌面云

通常交付流程是：准备安装包和基本数据—>硬件安装—>基础网络配置—>软件安装—>营业部部署。

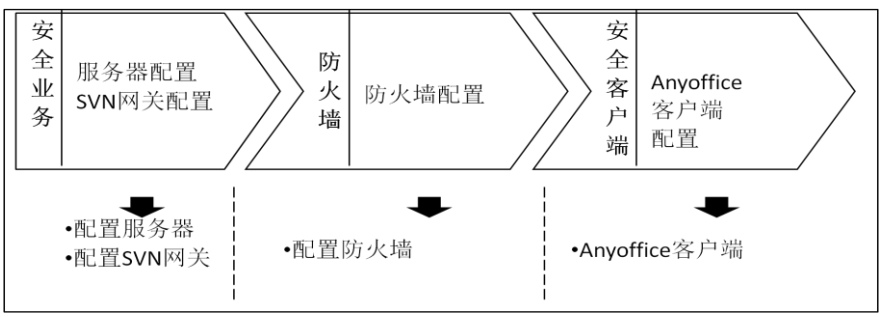
华为桌面云子解决方案开局流程如下：



- 离柜开户

通常交付流程是：业务服务器和SVN网关配置—>防火墙配置—> Anyoffice客户端配置。

华为离柜开户子解决方案开局流程如下：



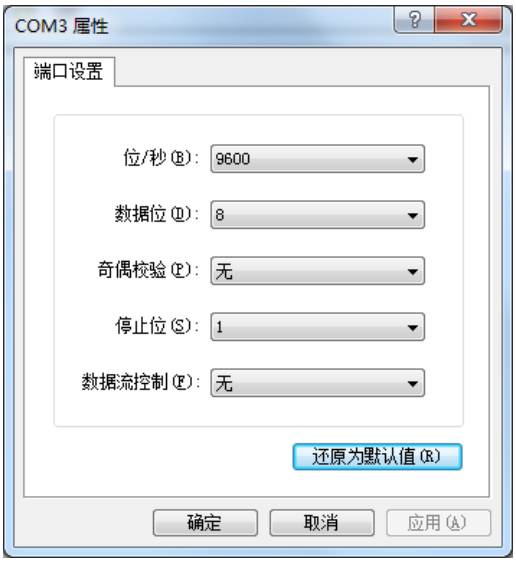
1.3 准备工作

- 证券一体机

  - 检查合同涉及的交付业务范围，针对每种业务列出一个交付清单。
  - 对于当前交付调试业务，检查交付清单中涉及的软硬件是否已经就绪。
  - 检查是否已经获取到当前项目的相关业务规划设计文档。
  - 检查当前交付业务的产品资料是否已经获取完全，如未获取请到华为官方网站下载。
  - 工具准备：PC一台，能够访问Internet，可以通过ipop远程ssh或telnet到营业部。
  - 软件准备：ftp或tftp （如涉及设备升级或补丁加载等需要使用ftp或tftp上传）。

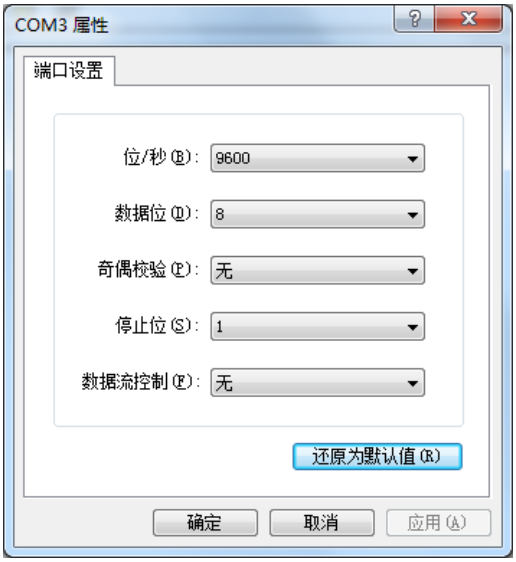
- 桌面云

  - 检查合同涉及的交付业务范围，针对每种业务列出一个交付清单。
  - 对于当前交付调试业务，检查交付清单中涉及的软硬件是否已经就绪。
  - 检查是否已经获取到当前项目的相关业务规划设计文档。
  - 检查当前交付业务的产品资料是否已经获取完全，如未获取请到华为官方网站下载。
  - 工具准备：笔记本电脑一台，并配有串口线和网线，使用超级终端链接设备的console端口进行调试，设置如下：（华为产品支持串口、web、telnet等方式进行配置，首次配置通常只能用串口）。



- 离柜开户

- 检查合同涉及的交付业务范围，针对每种业务列出一个交付清单。
- 对于当前交付调试业务，检查交付清单中涉及的软硬件是否已经就绪。
- 检查是否已经获取到当前项目的相关业务规划设计文档。
- 检查当前交付业务的产品资料是否已经获取完全，如未获取请到华为官方网站下载。
- 工具准备：笔记本电脑一台，并配有串口线和网线，使用超级终端链接设备的console端口进行调试，设置如下：（华为产品支持串口、web、telnet等方式进行配置，首次配置通常只能用串口）。



2 证券一体机

关于本章

介绍证券一体机解决方案的交付及配置过程。

2.1 U盘开局

本节主要介绍U盘开局完成的配置部分，包括营业部基础网络配置和营业部接入侧配置。

2.2 远程在线配置

本节主要介绍通过远程控制对轻型营业部进行配置。

2.1 U 盘开局

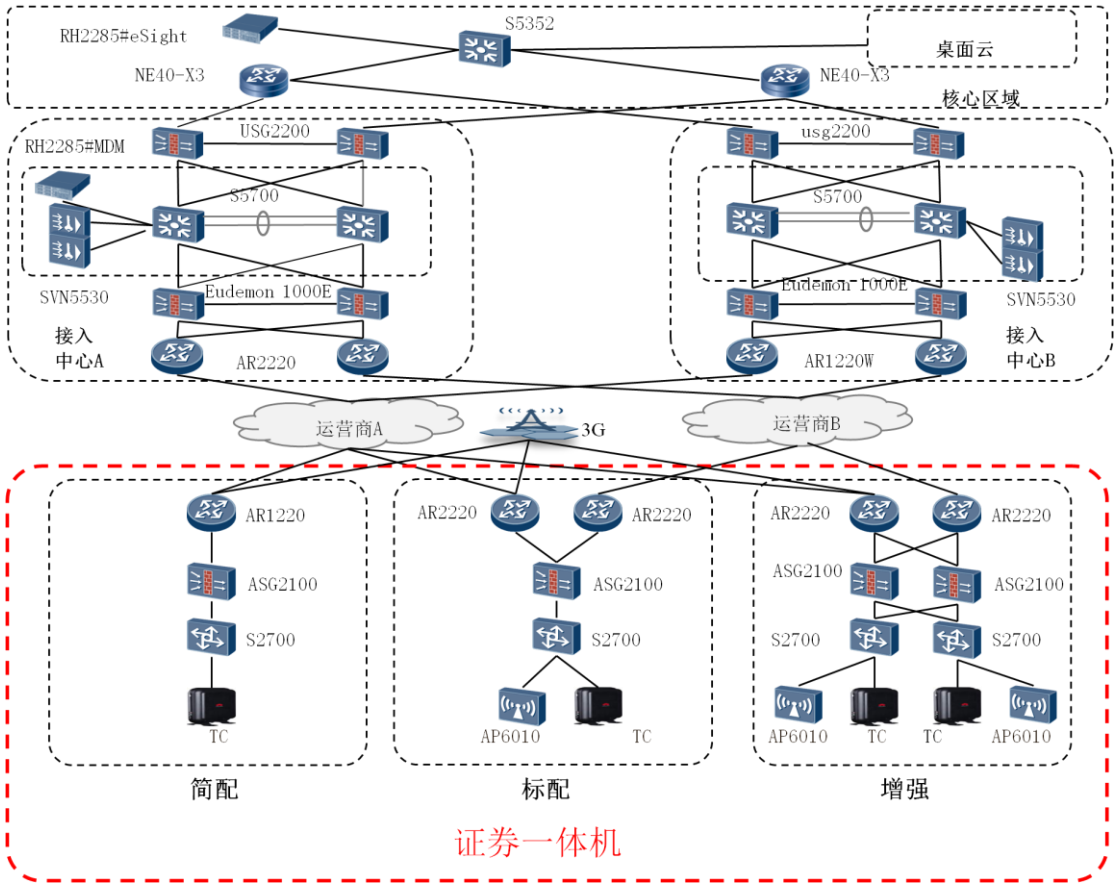
2.1.1 U盘开局模板修改

U 盘开局前需准备好开局文件，开局配置文件和索引文件根据附录中的模板进行修改，修改方法如下：

1. 模板中的配置文件必须修改的地方用##进行注释，请根据注释内容进行修改。
2. 模板中的配置文件非必改项及需要说明的地方，用#进行注释，可结合实际需要参照注释内容进行修改。
3. 模板中的开局索引文件用//进行注释，请根据注释内容进行修改，修改完成后务必删除//及注释内容。

2.1.2 证券一体机内部网络配置

2.1.2.1 组网需求



如上图所示，标配和增强型证券一体机组网部署中出口路由采用冗余备份，保证证券一体机的高可靠性。证券营业部网络可分为生产区、办公区等不同分区，不同分区之间网络不

能互通；业务PC和TC通过交换机接入，能够根据需要访问总部网络和Internet。

2.1.2.2 配置思路

1. 配置证券一体机各设备路由可达；
2. 配置ASG2100上行接口IP地址，及下行接口的2个vlan，并配置相应vlanif地址；2个vlan分别对应客户的生产网络和办公网络；
3. S2700上配置规划的区域的网络，使不同的终端接入不同的vlan，实现不同的业务功能；
4. 在2台AR路由器上配置VRRP，使2台AR路由器做双机热备。（适用于标配和增强型证券一体机）
5. 在2台ASG2100上配置HRP，使2台ASG2100做双机热备。（适用增强型证券一体机）
6. 配置WLAN，在路由器上配置好射频模板和ESS模板。

2.1.2.3 配置步骤

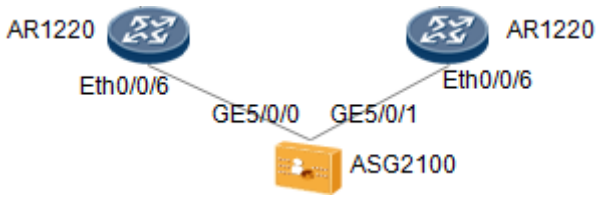
步骤1：证券一体机网元间路由可达

1） AR路由器与ASG2100间互通

AR路由器与ASG间采用三层逻辑接口(VLANIF)相连。IP网段规划为：

172.17.31.0/24

举例： ASG跟双AR路由器连接（以AR1220为例）



//AR1220#1接口配置

```
interface Vlanif31
 ip address 172.17.31.1 255.255.255.0  //三层逻辑接口VLANIF31
interface Ethernet0/0/6
 port link-type trunk
 port trunk pvid vlan 31
 port trunk allow-pass vlan 31 3561 to 3562 3570 //物理二层接口，跟ASG2100相连
```

//AR1220#2接口配置

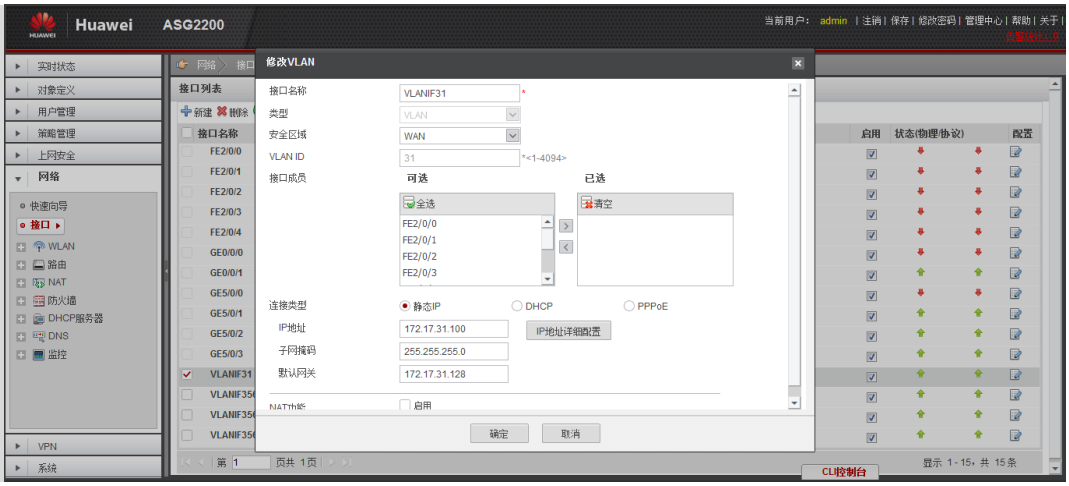
```
interface Vlanif31
 ip address 172.17.31.254 255.255.255.0  //三层逻辑接口VLANIF31
interface Ethernet0/0/6
 port link-type trunk
 port trunk pvid vlan 31
 port trunk allow-pass vlan 31 3561 to 3562 3570 //物理二层接口，跟ASG2100
```

//ASG2100的接口配置

a) 登录ASG2100的web界面

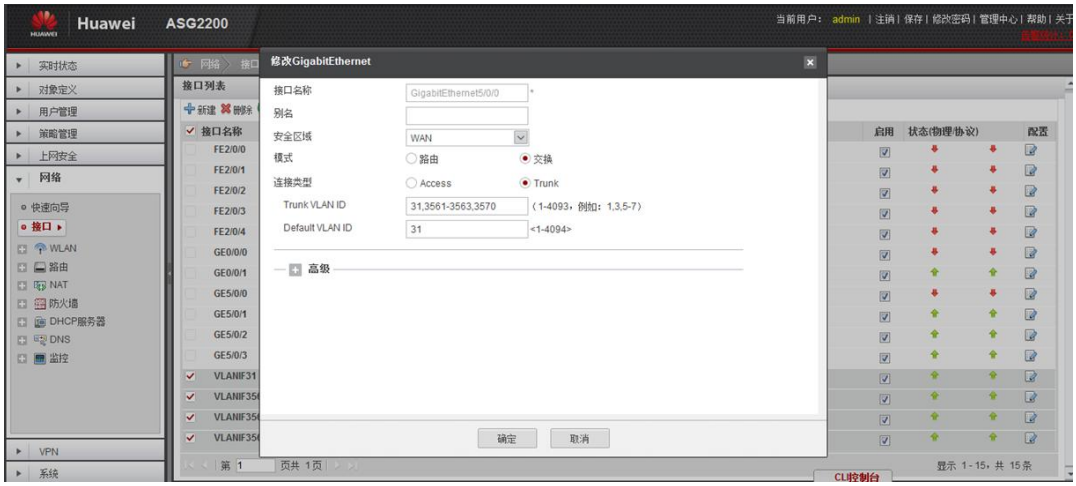
b) 选择网络->接口

c) 点击新建，按照下图所示填写，其他选项使用默认信息

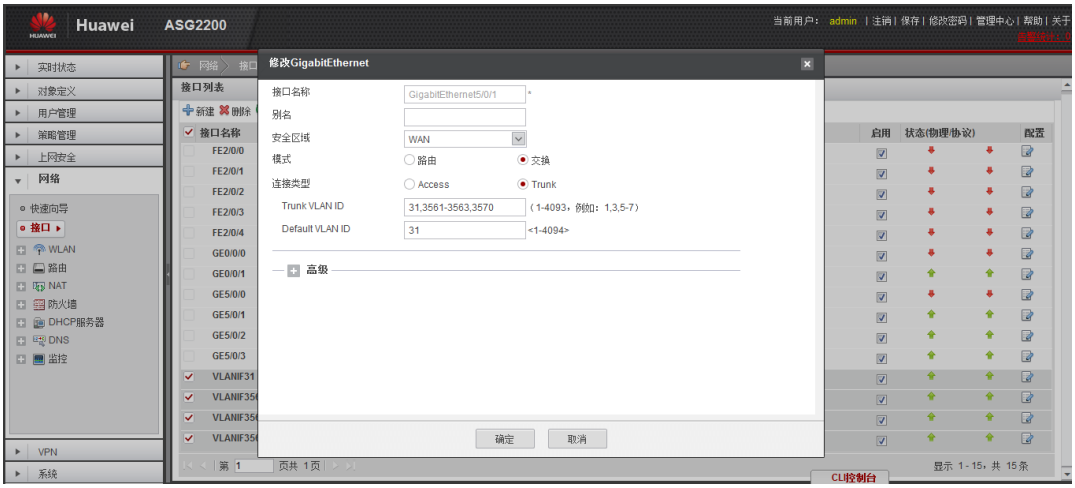


d) 选择网络->接口

e) 在接口列表中单击GigabitEthernet 5/0/0 所在行的  ，然后按照下图所示填写信息，其他使用默认信息。



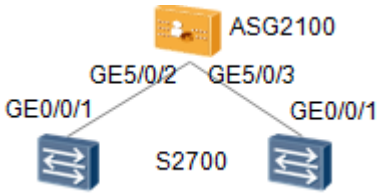
f) 在接口列表中单击GigabitEthernet 5/0/1所在行的  ，然后按照下图所示填写信息，其他使用默认信息。



2） ASG2100与S2700互通配置

ASG跟交换机间采用二层trunk方式连接。

举例：ASG与双交换机相连

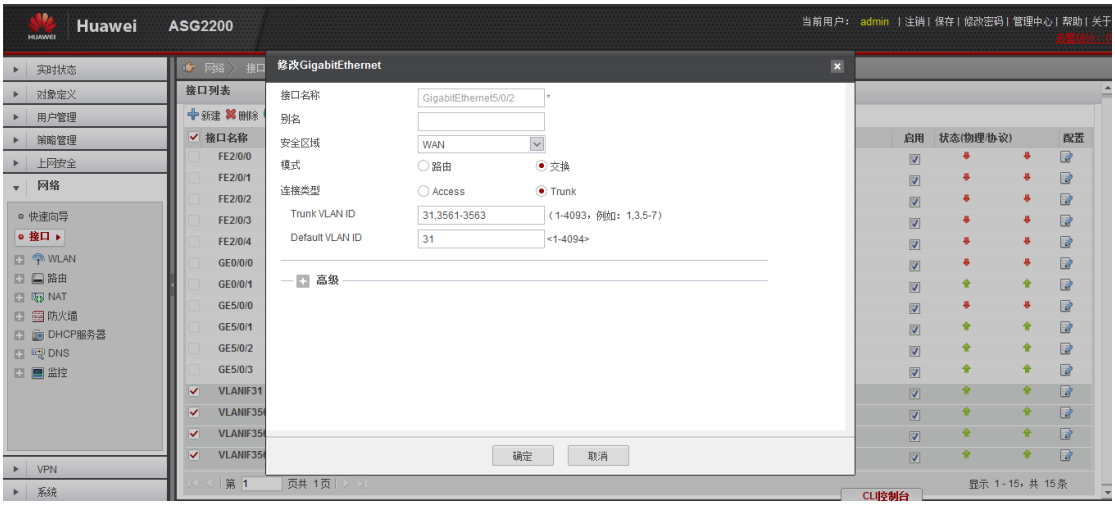


//ASG2100的接口配置

a） 登录ASG2100的web界面

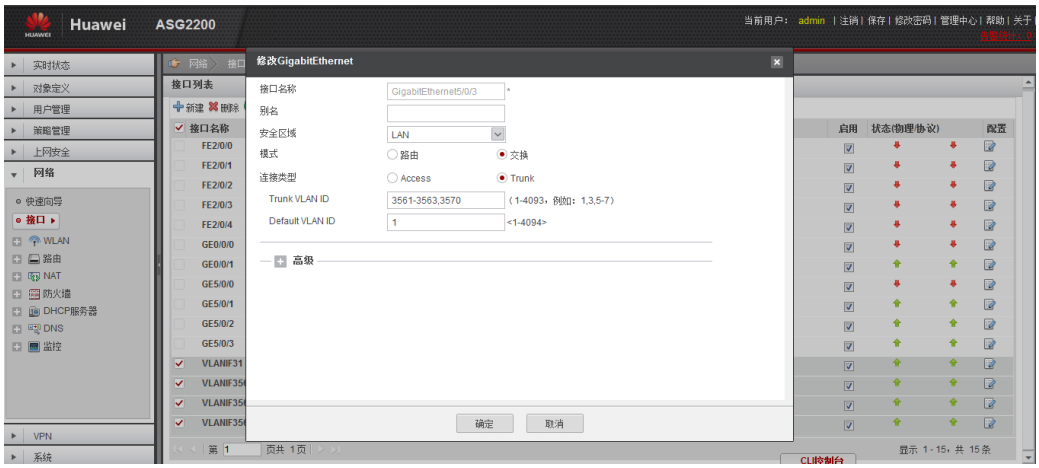
b） 选择网络->接口

c） 在接口列表中单击GigabitEthernet 5/0/2 所在行的  ，然后按照下图所示填写信息，其他使用默认信息。



d） 选择网络->接口

e） 在接口列表中单击GigabitEthernet 5/0/3 所在行的  ，然后按照下图所示填写信息，其他使用默认信息。



//交换机接口配置（两台S2700相同）

```
interface GigabitEthernet 0/0/1    //连接ASG2100
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3561 3562 3570
```

3） 网元间路由设置

举例：配置ASG跟AR路由器间路由可达

//AR1220#1路由配置

```
#    //配置AR1220#1到交换机（内网）的路由
ip route-static 172.18.0.0 255.255.0.0 172.17.31.100    //下一跳指向ASG2100
```

//AR1220#2路由配置

```
#    //配置AR1220#1到S2700（内网）的路由
ip route-static 172.18.0.0 255.255.0.0 172.17.31.100    //下一跳指向ASG2100
```

//ASG2100路由配置

下一跳地址为2台AR1220之间的vrrp的虚拟IP，vrrp配置请参照本节步骤5。

//S2700#1路由配置

```
#    //配置S2700#1的管理IP
interface Vlanif3561
 ip address 172.18.61.100 255.255.255.0
#    //配置S2700#1到AR1220(外网)的路由
ip route-static 0.0.0.0 0.0.0.0 172.18.61.1        //下一跳指向ASG2100
```

//S2700#2路由配置

```
#    //配置S2700#2的管理IP
interface Vlanif3561
 ip address 172.18.61.200 255.255.255.0
#    //配置S2700#2到AR1220(外网)的路由
ip route-static 0.0.0.0 0.0.0.0 172.18.61.1        //下一跳指向ASG2100
```

步骤2：营业部逻辑区域划分以及DHCP配置

1) 数据规划

区域	VLAN ID	工作模式	对应网段
生产区	3561	DHCP	172.18.61.0/24
办公区	3562	DHCP	172.18.62.0/24
管理区	3570	DHCP	172.18.70.0/24

2) 详细配置

逻辑区域的IP是ASG通过DHCP分配的，只需将PC接入交换机对应区域接口，就能自动获取该逻辑区域的IP。

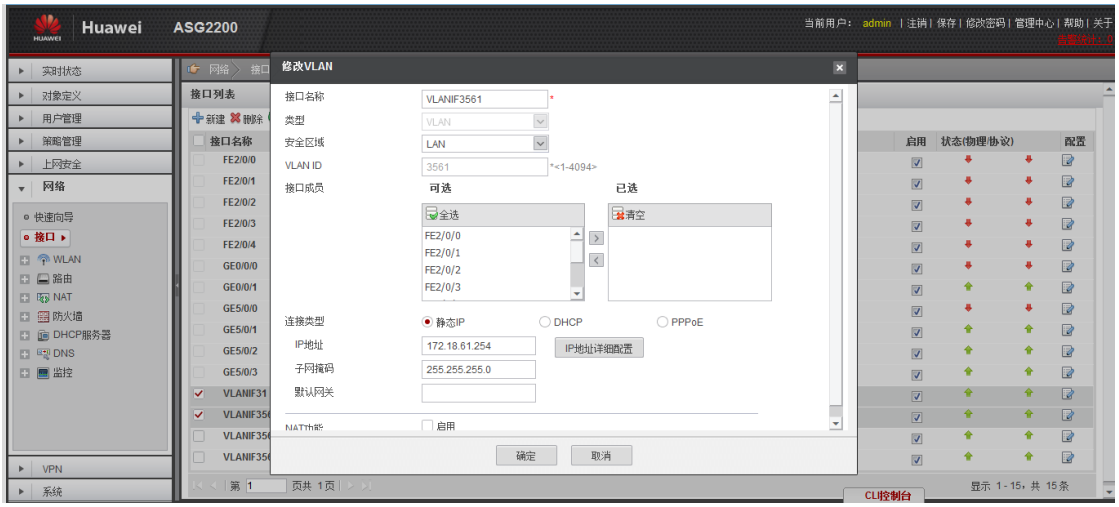
举例：配置开户区以及开启DHCP功能

//ASG2100业务规划

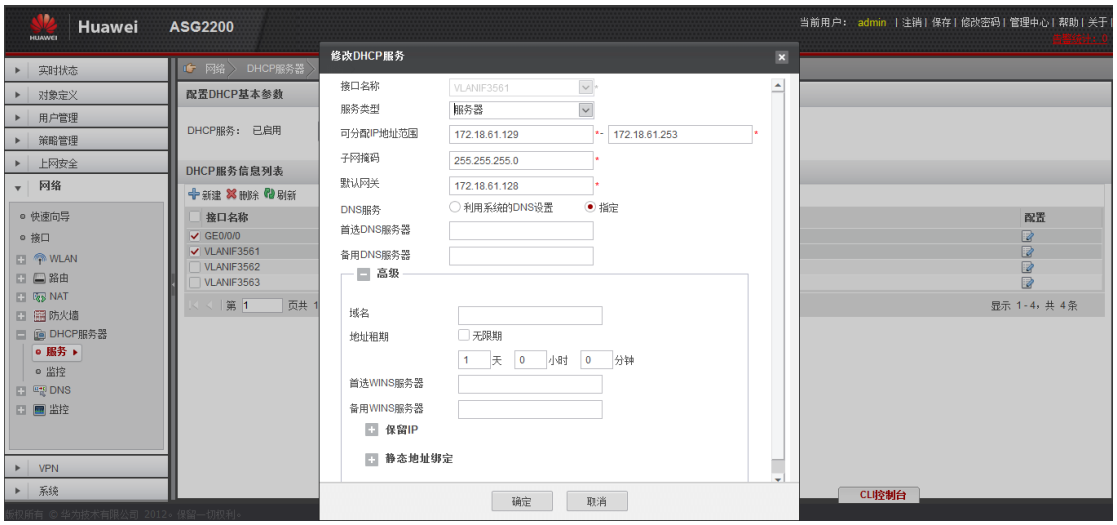
a) 登录ASG2100的web界面

b) 选择网络->接口

c) 点击新建，按照下图所示填写，其他选项使用默认信息



d) 启用DHCP功能。按照下图所示填写信息，其他使用默认信息



步骤3：营业部逻辑区域隔离

1) 区域隔离规划

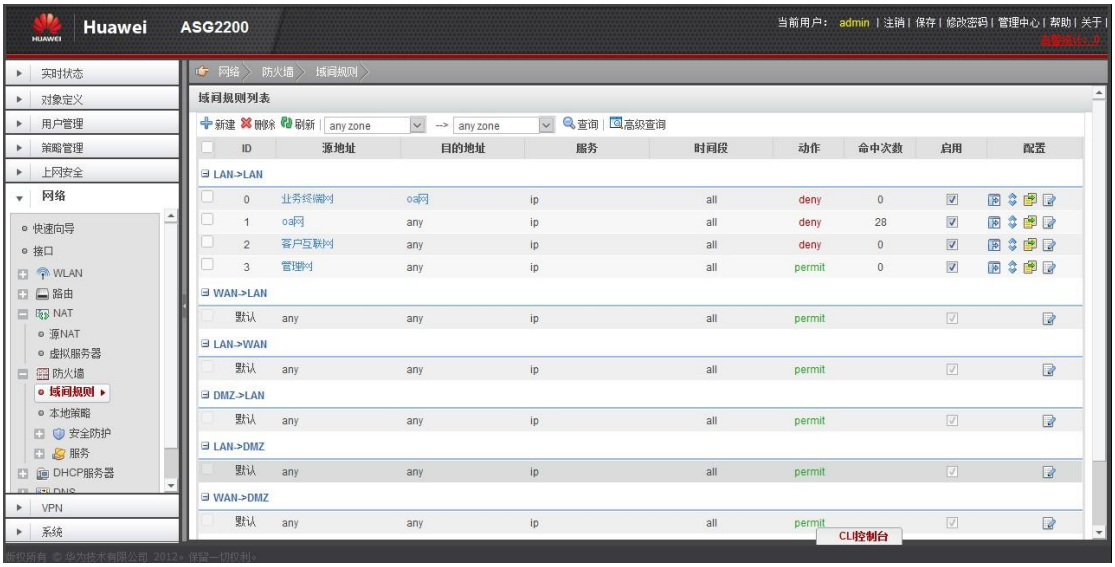
生产区和办公区不能互通。

2) 详细配置

区域之间的隔离可以根据实际需要进行调整。

举例：通过域间规则实现区域隔离

//在ASG上设置各个区域之间的互访操作权限



步骤4：划分交换机VLAN

举例：在S2700上创建vlan 3561、3562、3570

```
#
system
#
vlan batch 3561 3562 3570
#    //配置1号接口属于vlan3561，2-10号接口进行相同配置
interface Ethernet0/0/1
 port link-type access
 port default vlan 3561
#    //配置1号接口属于vlan3562，12-20号接口进行相同配置
interface Ethernet0/0/11
 port link-type access
 port default vlan 3562
```

步骤5：AR路由器双机热备（VRRP）

说明：此部分适用于证券标配和增强型一体机

为了保证当主路由器出现故障的时候，能及时切换到备用路由器上工作，需要在两台出口路由器上配置主备切换机制。

举例：AR1220的双机热备

1） 在AR1220#1(主路由器)上创建NQA探测

```
#
nqa huawei-instance test huawei
 huawei-type icmp
 destination-address ipv4 8.8.8.8    //探测地址为8.8.8.8，实际可改为探测总部出口IP
 frequency 10
start now
```

2) 在2台AR1220建创建vrrp

```
// AR1220#1
#
interface Vlanif31
 vrrp vrid 5 virtual-ip 172.17.31.128    //vrrp对外呈现的虚IP
 vrrp vrid 5 priority 120    //设置优先级为120
 vrrp vrid 5 preempt-mode timer delay 10    //设置抢占时间为10s
// AR1220#2
#
 interface Vlanif31
 vrrp vrid 5 virtual-ip 172.17.31.128
```

3) 在AR1220#1上应用vrrp与NQA联动

```
#
 interface Vlanif31
 vrrp vrid 5 track nqa test huawei reduced 40
```

步骤6：ASG双机热备（HRP）

说明：此部分适用于证券增强型一体机

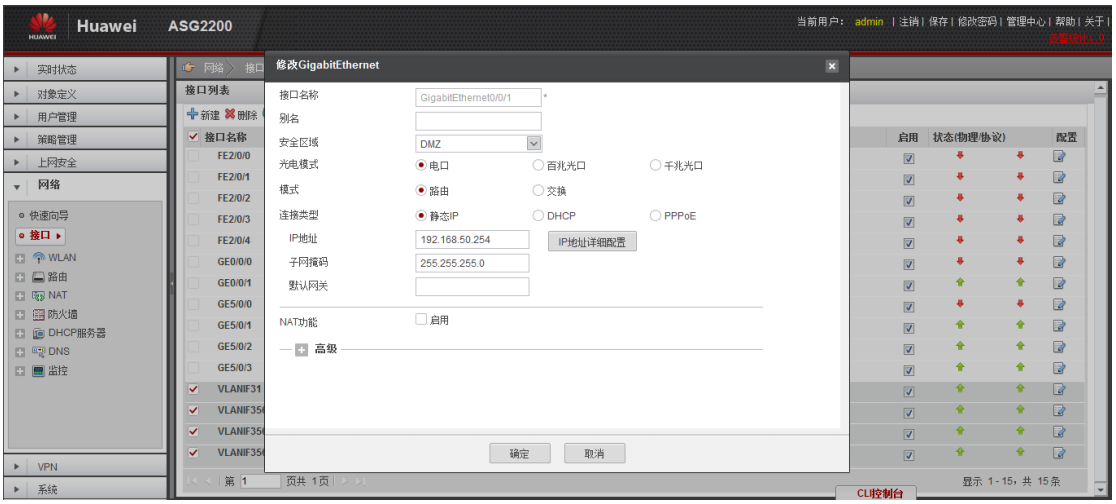
1) ASG2100#1

//启用HRP协议

a) 登录ASG2100 web界面

b) 选择网络->接口

c) 在接口列表中单击GigabitEthernet 0/0/1 所在行的  ，然后按照下图所示填写信息，其他使用默认信息。（心跳线）



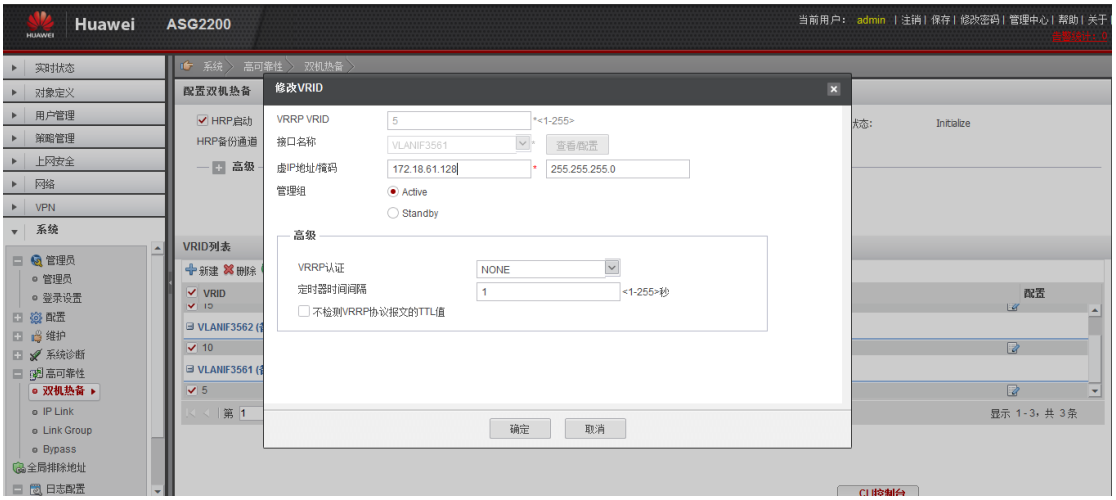
d) 选择系统->高可靠性->双机热备

e) 勾选HRP启动，并按照下图填写相关信息。

//配置VLANIF3561的VRRP

a) 选择系统->高可靠性->双机热备

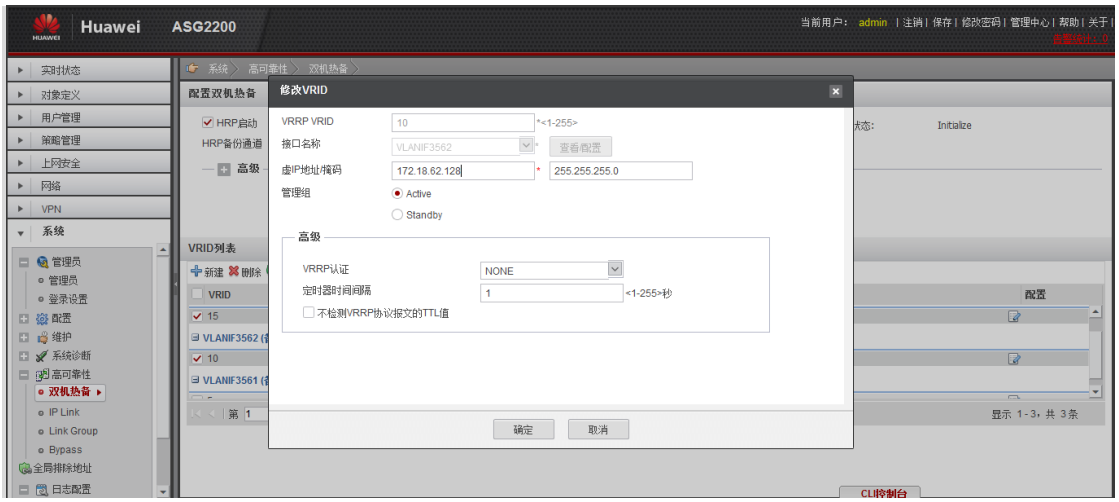
b) 在VRID列表中点击新建按钮，按照下图填写相关信息。



//配置VLANIF3562的VRRP

a) 选择系统->高可靠性->双机热备

b) 在VRID列表中点击新建按钮，按照下图填写相关信息。



2) ASG2100#2

//启用HRP协议

a) 登录ASG2100 web界面

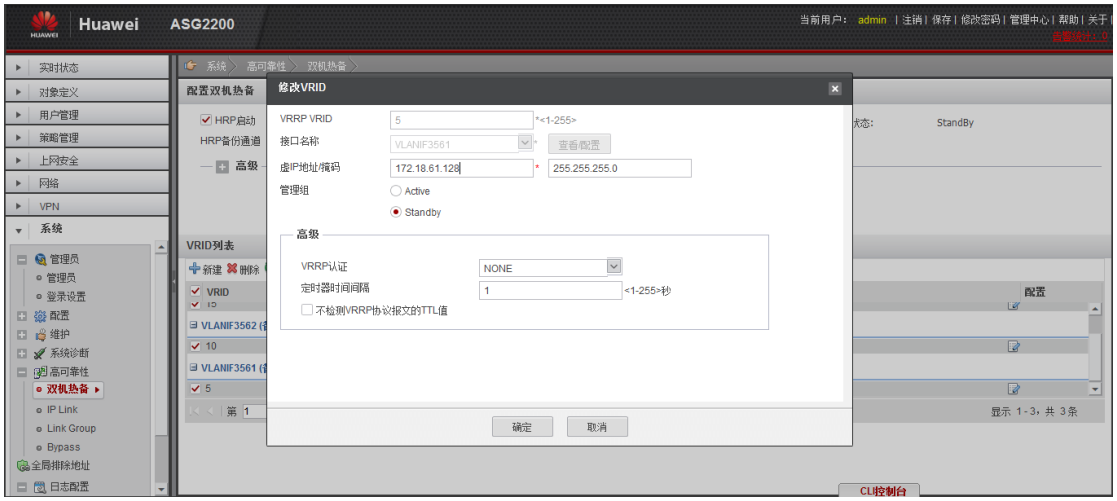
b) 选择系统->高可靠性->双机热备

c) 勾选HRP启动，并按照下图填写相关信息。

//配置VLANIF3561的VRRP

a) 选择系统->高可靠性->双机热备

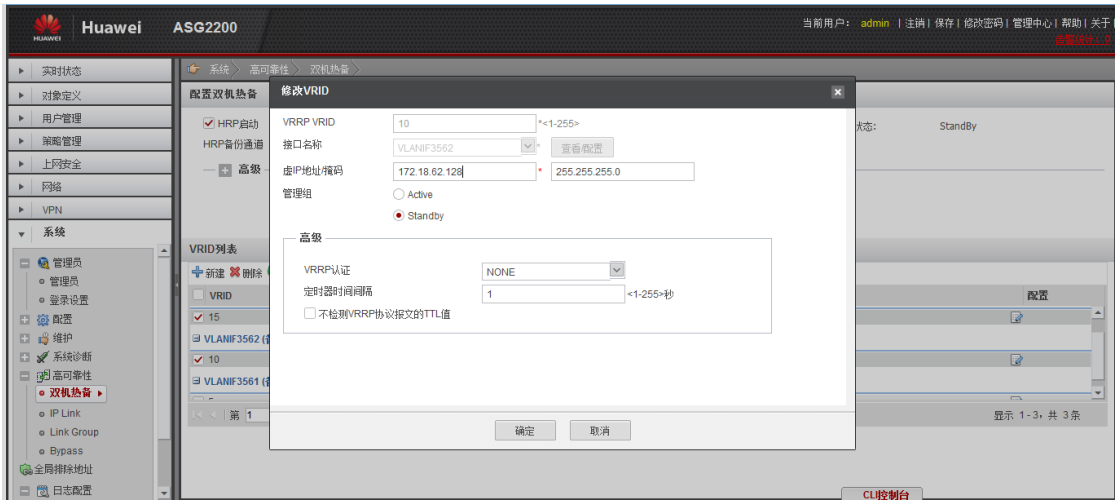
b) 在VRID列表中点击新建按钮，按照下图填写相关信息。



//配置VLANIF3562的VRRP

a) 选择系统->高可靠性->双机热备

b) 在VRID列表中点击新建按钮，按照下图填写相关信息。



步骤7：营业部wifi配置

举例：AR路由器作为AC的WIFI配置

```
#
dot1x enable    //使能dot1x
#
interface Wlan-Ess0  //定义一个供wifi接入的二层逻辑接口
 port hybrid tagged vlan 3561
#
wlan ac
 wlan ac source interface vlanif3570       //配置给AP分配IP的源地址
```

```
 ap-region id 5
 ap-auth-mode no-auth     //配置AP上线认证方式
 ap id 0 type-id 7 mac 5489-984e-5a07 sn AB38009004
wmm-profile name huawei-ap id 0     //定义WMM模板
 traffic-profile name huawei-ap id 0    //定义流量模板
 security-profile name huawei-ap id 0   //定义安全模板
  wep authentication-method shared-key  //采用wep认证+共享密钥
  wep key wep-104 pass-phrase 0 simple 8888888888888
 service-set name huawei id 0   //定义服务集
  wlan-ess 0
  ssid huawei-ap
  traffic-profile id 0
  security-profile id 0
  service-vlan 3561
 radio-profile name huawei-ap id 0
  wmm-profile id 0
 ap 0 radio 0
  radio-profile id 0
  service-set id 0 wlan 1
```

2.1.3 证券一体机外网接入配置

2.1.3.1 组网需求

参照2.1.2.1节，总部同营业部之间以ADSL作为主链路、3G作为备份链路互连，在链路上启用IPSec VPN，加密总部跟营业部间数据流的转发，保证数据流的安全可靠。

2.1.3.2 配置思路

1. 配置营业部端有线接入跟3G接入的路由，确保跟总部的接入点互通；
2. 配置营业部同总部间有线、3G的IPSec VPN隧道，加密需要保护的数据流；
3. 配置有线跟3G的切换策略，保证链路高可靠；

2.1.3.3 配置步骤

步骤1：ADSL接入配置

总部跟营业部间采用两条不同运营商的ADSL，保证链路的高可靠。

举例：AR1220有线接入配置

a） 创建acl，定义需要访问Internet的内网网段

```
acl number 3002      //定义需要访问internet的内网数据流
 rule 0 deny ip source 172.18.0.0 0.0.255.255 destination 10.0.0.0
0.255.255.255
 rule 5 permit ip source 172.18.61.0 0.0.0.255
 rule 10 permit ip source 172.18.62.0 0.0.0.255
 rule 15 permit ip source 172.17.31.0 0.0.0.255
```

b） 配置ADSL拨号

```
interface Dialer1
 link-protocol ppp
 ppp chap user 1301234567@163.gd     //配置ADSL拨号账号
 ppp chap password cipher 123456789     //配置ADSL拨号密码
 ppp pap local-user 1301234567@163.gd password cipher 123456789
 ppp ipcp dns admit-any
 ppp ipcp dns request
 tcp adjust-mss 1460
 ip address ppp-negotiate
 dialer user arweb
 dialer user 1
 dialer bundle 1
 dialer-group 1
 ipsec policy huawei
 nat outbound 3002
```

c） 将ADSL拨号应用于连接的物理接口上

```
//若ADSL为电话线，则接在ATM1/0/0上（ADSL板卡）
 interface atm1/0/0
 pppoe-client dial-bundle-number 1
//若ADSL为网线，则接在GE0/0/0上
 interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1
```

步骤2：3G接入配置

3G链路作为ADSL链路的备份，当两条ADSL链路都出现故障时，数据流可以通过3G链路与总部通讯。

举例：3G接入配置

//AR1220的3G接入配置（数据流同有线配置一致）

```
dialer-rule            //定义一个拨号规则
dialer-rule 1 ip permit
interface Dialer0
  link-protocol ppp
interface Cellular0/0/0
  link-protocol ppp     //链路协议PPP
  ppp chap user card     //用户名
  ppp chap password simple card      //密码
  ppp ipcp dns request      //配置DNS获取方式
  ip address ppp-negotiate          //3G的IP获取方式
  dialer enable-circular         //使能循环拨号
  dialer-group 1
  dialer timer autodial 15         //拨号超时时间设置
  dialer number *98# autodial     //联通拨号
  nat outbound 3001    //通过AR路由器的NAT，内网可以访问internet
  ip route-static 0.0.0.0 0.0.0.0 Cellular 0/0/0 preference 80    //路由
配置
```

步骤3：EPON接入配置

营业部通过光纤接入，需要使用EPON板卡。

举例：配置EPON接口的IP地址

```
system-view
 interface pon1/0/0
 ip address 1.1.1.1 255.255.255.0
```

步骤4：IPSec VPN配置

总部跟营业部间采用两条不同运营商的ADSL，保证链路的高可靠。同时，在链路上启用IPSec VPN，加密总部跟营业部间数据流的转发，保证数据流的安全可靠。

举例:有线接入的基于虚拟隧道的IPSecVPN配置，以AR1220#1为例

a) 采用动态密钥的方式建立IPSec VPN

```
//数据流定义
acl number 3001
 rule 5 permit ip source 172.18.0.0 0.0.255.255 destination 10.0.0.0 0.255.255.255
//创建IPSec 安全提议
ipsec proposal 1
 esp authentication-algorithm sha1
 esp encryption-algorithm aes-128
//创建IKE安全提议
ike proposal 1
 authentication-algorithm sha1
 encryption-algorithm 3des-cbc
 dh group2
 sa duration 3600
 authentication-method pre-share
// IKE对等体配置
ike peer 1 v1
 ike-proposal 1
 local-id-type name
 remote-name center
 dpd type periodic
 dpd msg seq-hash-notify
 remote-address 58.250.10.100
 pre-share-key 12345
//IPSec安全策略配置
ipsec policy huawei 10 isakmp
 security acl 3001
 ike-peer 1
 proposal 1
```

```
//在wan口运用ipsec策略
interface Dialer1
 ipsec policy branch1
//配置静态路由
 ip route-static 0.0.0.0 0.0.0.0 Dialer1
```

b) 采用证书认证的方式建立IPSec VPN

```
//数据流定义
acl number 3001
  rule 5 permit ip source 172.18.0.0 0.0.255.255 destination 10.0.0.0
0.255.255.255
//创建PKI实体
pki entity huawei
 country CN
 state guangdong
 organization huawei
 organization-unit info
 common-name hello
//创建PKI域
pki realm huawei
 entity huawei
 certificate-check none
pki realm default
 enrollment self-signed
//创建IPSec 安全提议
ipsec proposal 1
 esp authentication-algorithm sha1
 esp encryption-algorithm aes-128
//创建IKE安全提议
ike proposal 1
 authentication-algorithm sha1
 encryption-algorithm 3des-cbc
 dh group2
```

```
 sa duration 3600
 authentication-method rsa-signature
// IKE对等体配置
ike peer 1 v1
 ike-proposal 1
 local-id-type name
 remote-name cluster-zt
 dpd type periodic
 dpd msg seq-hash-notify
 remote-address 58.250.10.100
 pki realm huawei
//IPSec安全策略配置
ipsec policy huawei 10 isakmp
 security acl 3001
 ike-peer 1
 proposal 1
//在wan口运用ipsec策略
interface Dialer1
 ipsec policy branch1
//配置静态路由
 ip route-static 0.0.0.0 0.0.0.0 Dialer1
```

c） 3G接入的IPSec VPN配置

总部跟营业部间采用两条不同运营商的ADSL，保证链路的高可靠。同时，在链路上启用IPSec VPN，加密总部跟营业部间数据流的转发，保证数据流的安全可靠。

说明：IPsec VPN具体配置跟有线接入IPSec VPN配置一样,配置完成后在3G接口上运用ipsec策略即可。

```
#
interface Cellular0/0/0
ipsec policy branch1
```

步骤5：有线与3G切换

1） 为了保证链路可靠，在两条ADSL有线接入故障的时候，必须能自动切换到3G。同时为保证链路的质量，当有线恢复正常的时候，数据流能自动切换到有线。

举例：有线跟3G的主备倒换

//为了探测链路是否故障，需要通过NQA的ICMP报文监测

```
nqa test-instance user test
  test-type icmp
  destination-address ipv4 202.96.134.134      //探测的公网IP
  frequency 20                                 //探测频率
  probe-count 2
  start now
interface Cellular0/0/0
  standby track nqa user test                  //探测失败，启动3G链路
```

//通过配置3G路由优先级高于有线，当3G链路UP的时候，数据流从3G转发

```
ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0 172.17.33.200
preference 150
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/0 preference 80
ip route-static 8.8.8.8 255.255.255.255 GigabitEthernet0/0/0
172.17.33.200
```

2.2 远程在线配置

2.2.1 通过SSH工具进行配置

通过SSH工具下发AR路由器所需CA证书和local证书并激活。

2.2.1.1 配置思路

1. 通过SSH工具远程连接AR路由器；
2. 通过ftp服务将CA证书、local证书上传到AR路由器；
3. 激活证书文件,建立起总部和营业部间的IPsec VPN通讯链路；

2.2.1.2 配置步骤

步骤1：通过ftp上传证书文件到AR路由器

方法1：AR作为ftp client

1) 渠道商从客户处获取证书文件，包括CA证书（如：internal_ca.crt）和local(如vpn-01.p12)证书及营业部IP地址。
2) 创建ftp服务器，将证书文件放在ftp指定目录下。
   说明：ftp服务器需配置公网IP，确保AR路由器可以通过ftp连接到服务器。
3) 在ftp服务器上，通过SSH工具连接AR路由器。
4) 在AR路由器上连接ftp服务器，获取文件。

```
<AR#2>ftp 172.18.61.132
Trying 172.18.61.132 ...
Press CTRL+K to abort
Connected to 172.18.61.132.
220 FTP Server ready.
User(172.18.61.132:(none)):huawei
331 Password required for huawei.
Enter password:
230 User huawei logged in.
```

```
[AR#2-ftp]get vpn-01.p12
200 Port command successful.
150 Opening data connection for vpn-01.p12.
226 File sent ok
FTP: 2615 byte(s) received in 4.595 second(s) 569.09byte(s)/sec.

[AR#2-ftp]get internal_ca.crt
200 Port command successful.
150 Opening data connection for internal_ca.crt.
226 File sent ok
FTP: 1076 byte(s) received in 4.684 second(s) 229.71byte(s)/sec.
```

参照以上操作将2台AR路由器所需的证书文件分别上传到2台AR路由器上。

方法2：AR作为ftp server

1) 在AR上开启ftp server，配置ftp目录及ftp登录用户。

```
#
ftp server enable
 set default ftp-directory flash:/
#
aaa
local-user root password cipher %$%$U+88&ZPxn0o(0#7Ln-GFM]^#%$%$
 local-user root privilege level 15
 local-user root ftp-directory flash:/
 local-user root service-type ftp
```

2) 在操作终端上使用命令行加载。

```
D:\ftp> ftp 10.164.30.20（此处假设营业部AR的外网IP为10.164.30.20）
Connected to 10.164.30.20.
220 FTP service ready.
User(10.164.28.20:(none)):root  # 手工输入用户名，回车
331 Password required for root.
Password:  # 输入密码admin，回车，密码不会显示在屏幕上
230 User logged in.
ftp> binary
200 Type set to I.
ftp> put vpn-01.p12
200 Port command okay.
150 Opening binary mode data connection for vpn-01.p12
226 Transfer complete.
ftp: 发送 2615 字节，用时 275.39Seconds 251.02Kbytes/sec.
ftp> put internal_ca.crt
200 Port command okay.
150 Opening binary mode data connection for internal_ca.crt
226 Transfer complete.
ftp: 发送 1076 字节，用时 275.39Seconds 251.02Kbytes/sec.
```

参照以上操作将2台AR路由器所需的证书文件分别上传到2台AR路由器上。

步骤2：激活并校验证书

1） 激活证书：

- 激活 CA 证书

此处证书文件名需和客户提供的证书一致，PKI 域（test）需与 AR 路由器中配置的 PKI 域一致。

```
[AR#2]pki import-certificate ca test pem
Please enter the name of certificate file <length 1-127>: internal_ca.crt
 The CA's Subject is O=cczq-h25t6e5zy2..z6oxo6,
 The CA's fingerprint is:
   MD5  fingerprint: 7091ee26  ee7340bc  25c1e952  cb29c822
   SHA1 fingerprint: 5b9e10e5  174742b5  fc03b98d  71ca08e1  ef0d84be
 Is the fingerprint correct? [Y/N]: y
Successfully imported the certificate.
```

- 激活 local 证书

此处证书文件名和密码需和客户提供的证书一致，PKI 域（test）需与 AR 路由器中配置的 PKI 域一致。

```
[AR#2]pki import-certificate local test pkcs12
Please enter the name of certificate file <length 1-127>: vpn-01.p12
You are importing a local certificate, the current private key is required.
Please enter the name of private key file <length 1-127>: vpn-01.p12
Please enter the type of private key file(pem , p12): p12
The current password is required, please enter your password <length 1-31 >:***
***
Successfully imported the certificate.
```

2) 校验证书状态

- 校验CA证书状态

此处PKI域（test）需与AR路由器中配置的PKI域一致。

```
[AR#2]pki validate-certificate ca test
 Serial Number:
   01
 Issuer:
   O=cczq-h25t6e5zy2..z6oxo6
 Subject:
   O=cczq-h25t6e5zy2..z6oxo6
Verify result: the certificate is good.
```

- 校验local证书状态

此处PKI域（test）需与AR路由器中配置的PKI域一致。

```
[AR#2]pki validate-certificate local test
 Serial Number:
   14 8d
 Issuer:
   O=cczq-h25t6e5zy2..z6oxo6
 Subject:
   O=cczq-h25t6e5zy2..z6oxo6
   OU=users
   CN=cczq-vpn-01
Verify result: the certificate is good.
```

步骤3：查看Ipsec VPN状态

在用户视图下，通过display ike sa 命令查看IPsec VPN是否已经建立成功。

```
<AR1200#1>dis ike sa
   Conn-ID  Peer            VPN   Flag(s)                 Phase
  -----------------------------------------------------------------
        4    58.251.17.100   0     RD|ST                   2
        3    58.251.17.100   0     RD|ST                   2
        2    58.251.17.100   0     RD|ST                   2
        1    58.251.17.100   0     RD|ST                   1

  Flag Description:
  RD--READY    ST--STAYALIVE    RL--REPLACED    FD--FADING    TO--TIMEOUT
  HRT--HEARTBEAT    LKG--LAST KNOWN GOOD SEQ NO.    BCK--BACKED UP
```

2.2.2 通过统一网管进行配置

通过统一网管添加证券一体机网元，激活AR路由器路由的AC License并将AR路由器设置为AC模式；部署AP并配置上网行为管理。

2.2.2.1 组网需求

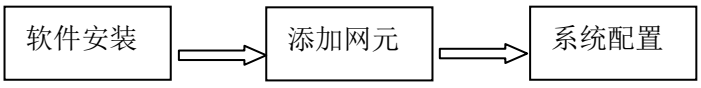
参照2.1.2节组网模型，通过统一网管对证券一体机AR路由器、ASG2100、S2700交换机、AP等网元进行管理和配置。

2.2.2.2 配置思路

1) 安装eSight,按照配置手册添加网元，完成基础配置。使渠道商可以通过eSight统一网管对各网元进行配置。
2) 通过eSight配置WLAN，将AP绑定AC并将射频模板和ESS模板部署到AP。
3) 激活ASG2100的license，配置上网行为管理策略，并应用策略到用户。

2.2.2.3 配置步骤

步骤1：eSight安装及基础配置



eSight软件安装和基础配置请参照eSight产品文档，链接如下：

http://support.huawei.com/enterprise/productsupport?pid=6725036&idAbsPath=7919710|9856717|7923123|9858904|6725036

步骤2：配置WLAN

1) 激活AR路由器上AC license

渠道商通过合同号从华为指定网站获取license文件后，通过eSight登录AR路由器的web界面，在系统管理>license管理菜单下，从本地读取license文件并激活。

2) 设置AR路由器WLAN功能为AC工作模式

通过eSight进入AR路由器的telnet窗口。

在系统视图下执行命令：`set workmode wlan ac`

```
<AR1200#1>system
Enter system view, return user view with Ctrl+Z.
[AR1200#1]set work wlan ac
WARNNING: The WorkMode Change will be activated after board reboot. Continue? [y
/n]:y
[AR1200#1]
```

重启AR路由器，使配置生效。

```
[AR1200#1]quit
<AR1200#1>reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration.
Continue ? [y/n]:n
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
<AR1200#1>
```

2台AR路由器都分别需要执行以上操作。

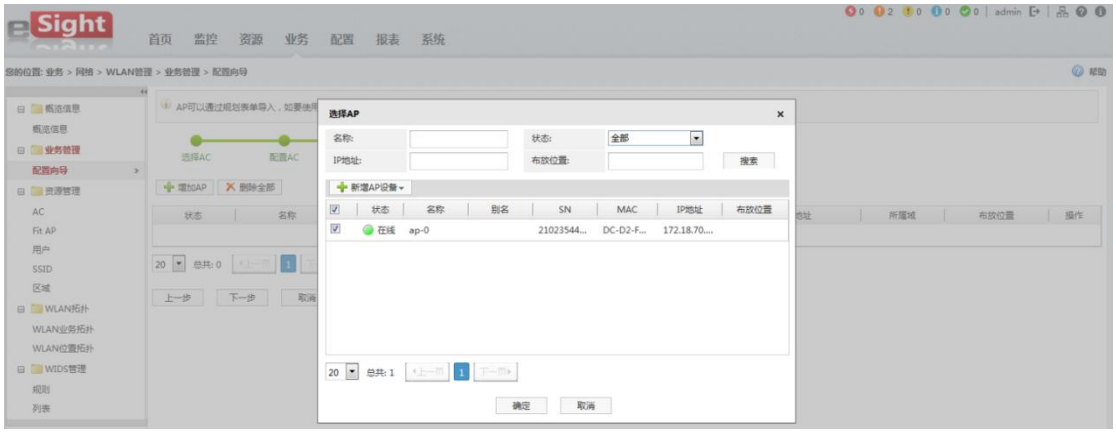
说明：在AR路由器重启时，有2次交互选择。第一次选择“n”,第二次选择“y”。

3） 部署AP

登录eSight,在eSight的“业务> 网络>WLAN管理>业务管理>配置向导”界面下，选择AC后点击“下一步”

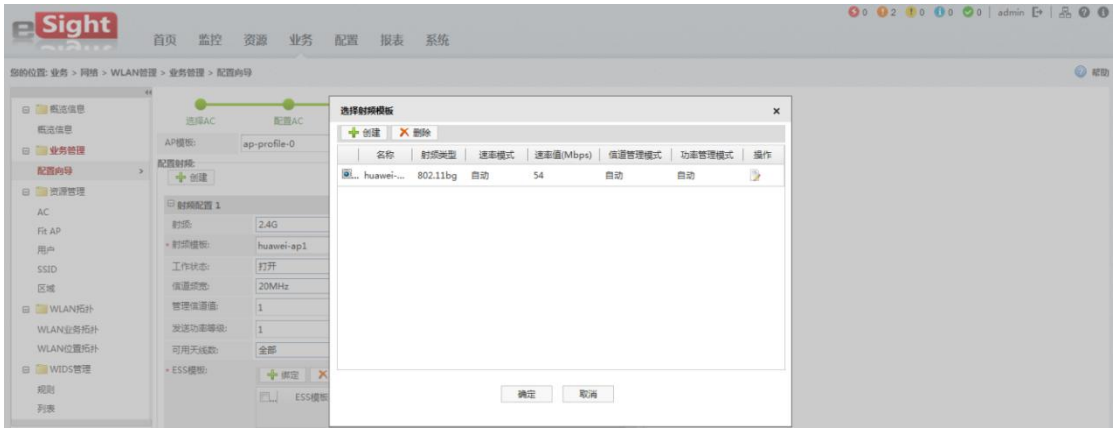
参照下图配置接口参数，点击“下一步”

参照下图选择AP后，点击“下一步”

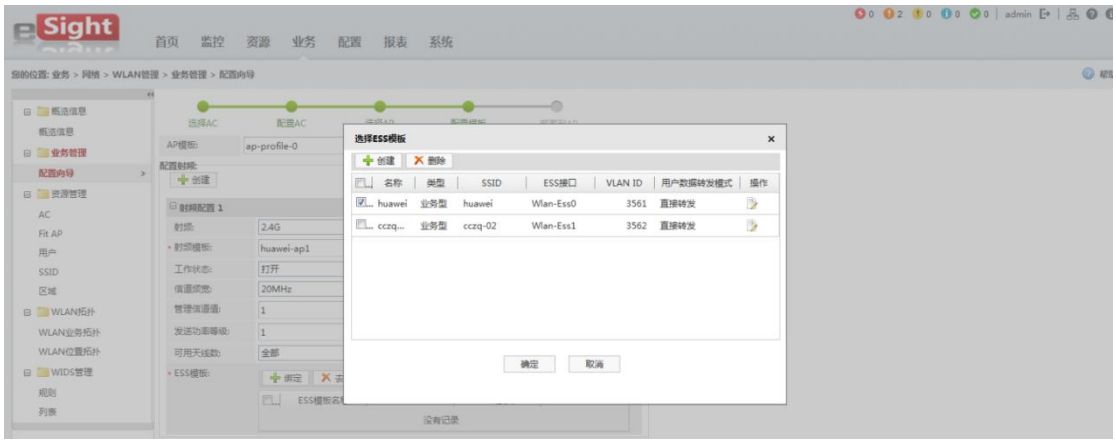


参照下图点击“下一步”

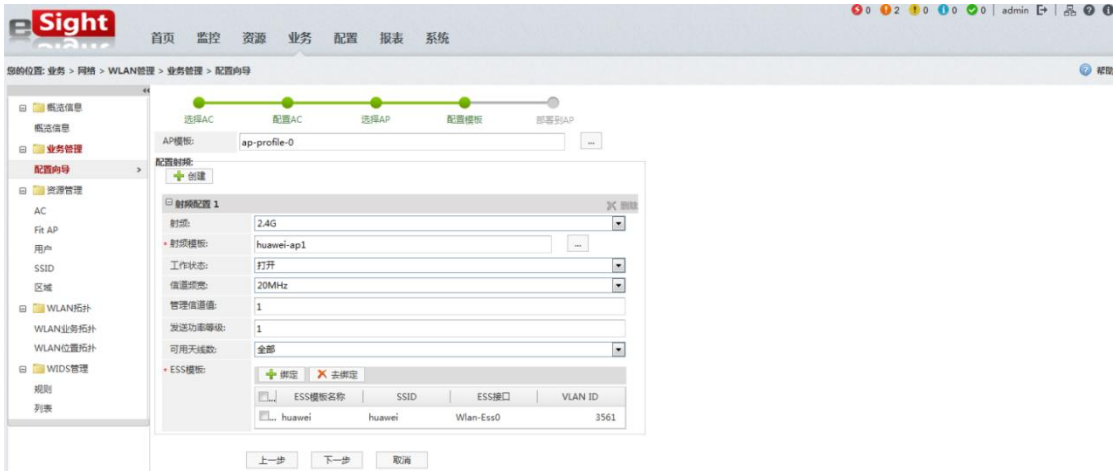
参照下图选择射频模板后，点击“确定”



参照下图选择ESS模板后，点击“确定”



参照下图点击“下一步”



参照下图点击“部署”，完成AP部署。

步骤3：营业部上网行为管理配置

1） 获取ASG2100 License授权编码（LAC）。（若无license文件，直接忽略此步骤）

在发货附件中找到License授权证书，并获取LAC，如下图所示。

说明：License授权证书以纸面件（A4大小）或CD件的方式随产品一起提供给客户。

Serial No.:

LICENSE CERTIFICATE

This License Certificate is issued to the Authorized User of Huawei Products. This License Certificate records License Authorization Code (LAC), which is for the purpose of application for and access to the electronic license file for equipment installation. Prior to equipment installation, the Project Supervisor of Huawei needs to obtain the LAC, with which the Project Supervisor will then provide electronic license file for equipment installation. In case that LAC does not work due to modification thereto, the Project Supervisor will regain the new LAC in accordance with contract, and then provide the electronic license file.

Contract Information

Contract No.:
Order No.:
Entitlement ID(LAC):
Installation site:

Authorized User Information

Customer No.:
Customer Name:

Products with License

Product Name	Version	Quantity	Period of Validity
		1	PERMANENT

2） 申请License文件。（若无license文件，直接忽略此步骤）

说明：本地手动激活License时需要申请，在线激活不需要申请，推荐直接连接License中心在线激活。

a） 获取ESN。

ESN标签位于设备机箱后面板的左上角，TYPE和S/N组合在一起构成ESN，例如210235G6HQZ0B6000058。

b） 获取License文件。

注意：如果为多台设备申请License，请确保每台设备的LAC与ESN一一对应。将LAC和ESN发送到邮箱license@huawei.com。技术支持工程师收到您的邮件后会尽快处理，并将License文件发送到您的邮箱。如果您无法及时获取到License文件，请联系客户服务处理，电话为4008229999。

3） 激活License。 （若无license文件，直接忽略过此步骤）

选择“系统 > 维护 > License管理”，单击“激活”图标。

a） 在线自动激活（需要确保设备可以访问Internet）

输入LAC，License中心域名使用缺省值，单击“激活”。

b） 本地手动激活（必须申请License文件）

选择申请的License文件，单击“激活”。

说明：只有当ASG的设备序列号完全与当前License文件（*.dat）匹配时，当前License文件才能成功被激活。

系统中只能存在一个处于激活状态的License文件，激活新的License将会使旧的License失效。

4） 配置上网行为管理策略

上网行为管理策略配置请参照ASG2100产品文档，连接如下：

http://support.huawei.com/ehedex/hdx.do?docid=DOC1000003304&lang=zh

3 桌面云

关于本章

介绍桌面云的安装配置。

3.1安装准备

本节主要介绍安装前的准备工作。

3.2交换机配置

本节主要介绍交换机的配置。

3.3软件安装

本节主要介绍桌面云系统的安装。

3.4营业部部署

本节主要介绍营业部终端的安装部署。

3.1 安装准备

请参照FusionAccess产品文档

FusionAccess（V100R005C00）

3.2 交换机配置

交换机配置请参照2.1.2.3节步骤5。

3.3 软件安装

请参照FusionAccess产品文档

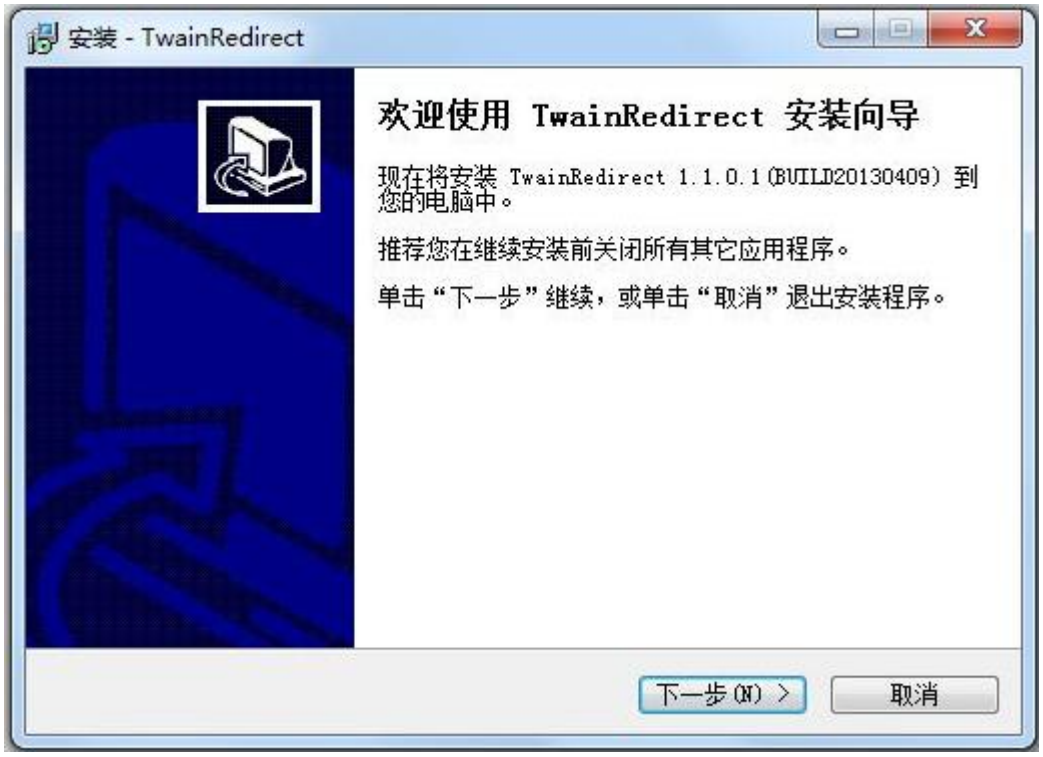
FusionAccess（V100R005C00）

3.4 营业部部署

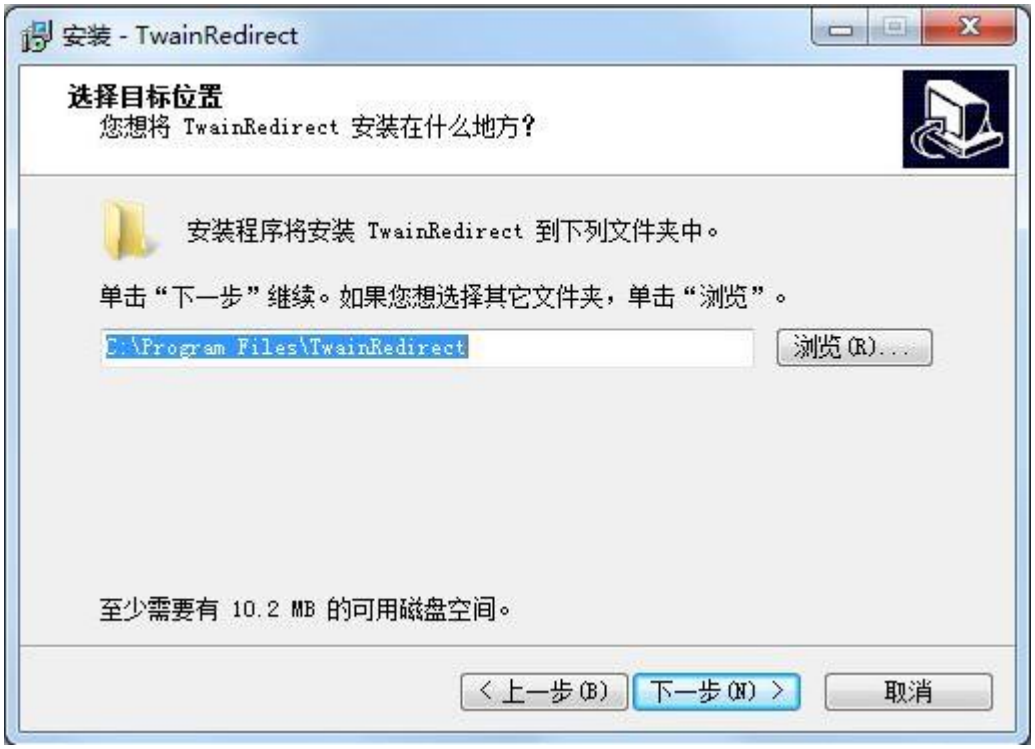
将营业部所需外设（如：高拍仪、身份证读卡器）连接在TC上，通过AD服务器分配的桌面云账号登录桌面云，安装桌面云外设兼容性补丁。

双击打开桌面云外设兼容性补丁程序：

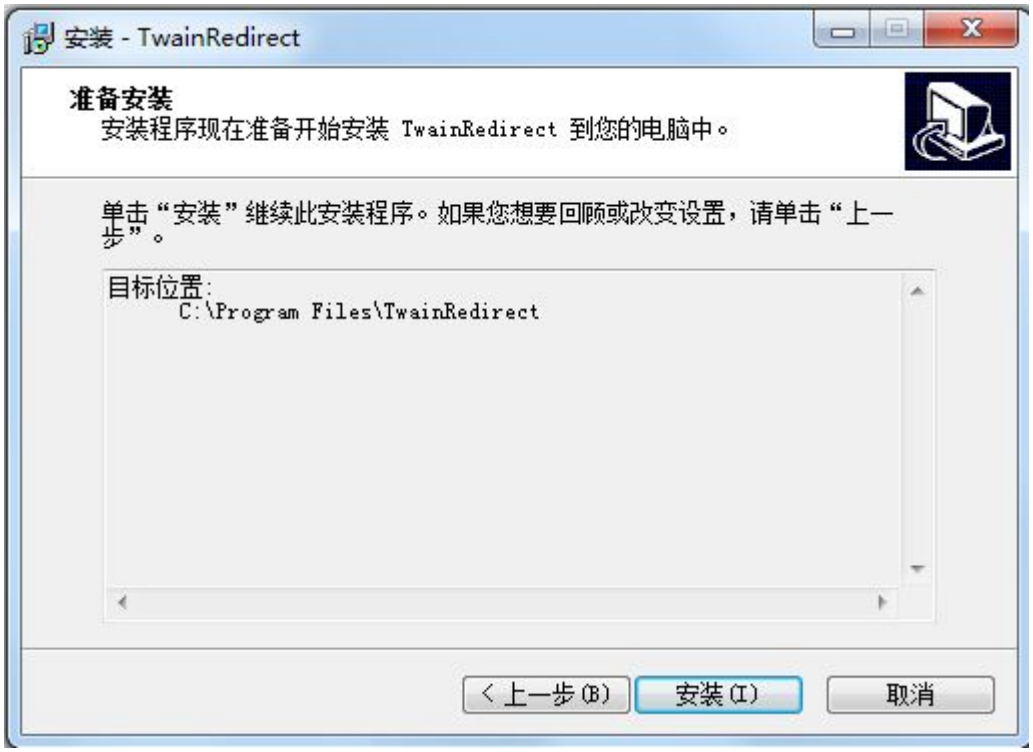
点击“下一步”

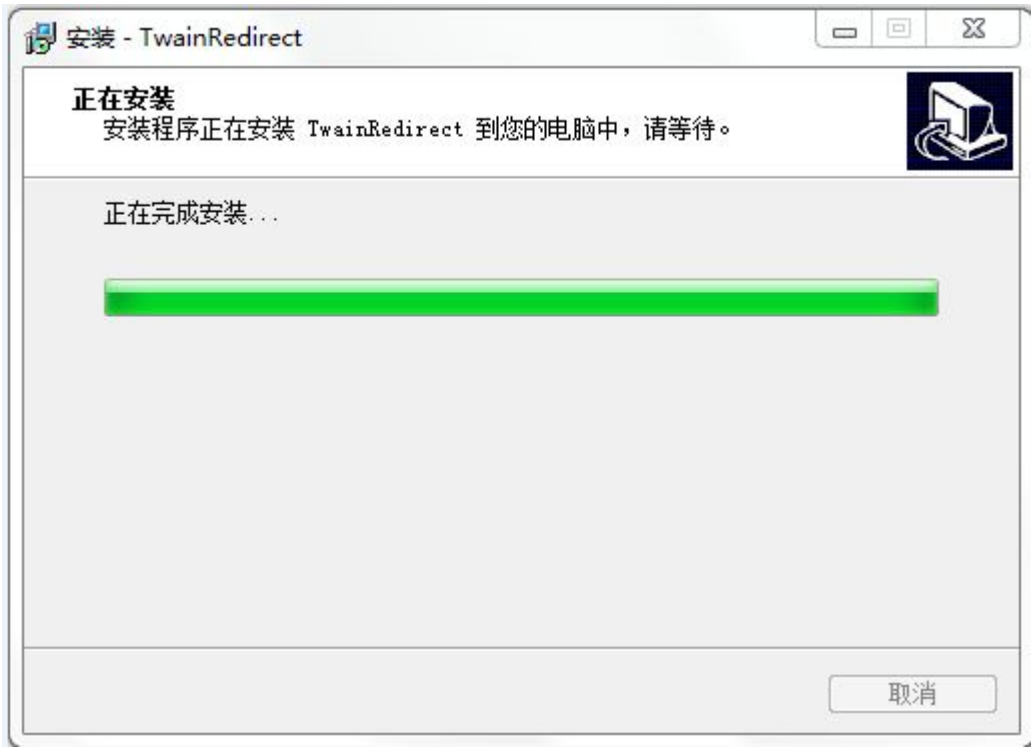


选择安装路径后，点击“下一步”



点击“安装”





安装完成后，选择“立即重启电脑”后，点击“完成”，等待虚拟机重启完成后，重新登录即可。

4 离柜开户

关于本章

介绍本立柜开户解决方案的配置过程。

4.1 安全业务

本节主要介绍MDM服务器和安全网关的配置。

4.2 防火墙配置

本节主要介绍防火墙的配置。

4.3 安全客户端配置

本节主要介绍Anyoffice的配置。

4.1 安全业务

4.1.1 MDM服务器配置

请参照Anyoffice产品文档

Anyoffice (V200R002C10)

4.1.2 配置安全网关

请参照 SVN2006产品文档

SVN2260（V200R001C01）

4.2 防火墙配置

请参照USG2000产品文档

USG2260（V300R001）

4.3 安全客户端配置

正确配置移动客户端的AnyOffice后，终端用户才能使用安全邮箱、安全浏览器和MDM业务。下面以苹果iPad接入为例介绍配置方法，其它终端类似。

举例：

1. 移动终端WLAN热点接入。

   要保证移动终端正常接入，前提条件是移动终端通过wifi获取的动态IP地址中含有DNS的IP地址，否则苹果终端无法使用无线热点。热点输入的用户名和密码来源于WLAN配置的用户名与密码。

2. AnyOffice配置

在移动终端上点击客户端AnyOffice的图标进入登录界面。配置登录的用户名与密码。以byod4账号为例配置步骤如下:

在AnyOffice的登录界面右上角点击配置按钮，进入到系统配置。在系统配置界面SVN的网关地址，端口。IP地址即为虚拟网关的IP地址（如：172.21.32.96），端口默认设置为443。邮箱地址设置的登录名与用户登录账号一致。

设置完成后再回到登录界面，点击登录进入到安全工作台界面。SVN安全网关和MDM服务器会对客户端账号进行认证、对移动终端做准入检查，AnyOffice登录成功后的安全邮箱业务、安全浏览器、安全平台、终端设备系统和终端应用会受策略组各项策略限制。

5 数据中心网络接入配置

关于本章

介绍数据中心网络接入配置流程，使营业厅能与数据中心网络接入区通过IPSEC通信，包括IPSec VPN的配置以及接入中心的路由、防火墙主备功能等。

5.1 组网需求

本节主要介绍营业部跟数据中心网络接入区连接需求以及接入中心的组网需求。

5.2 配置思路

本节主要介绍接入中心的IPSec VPN配置以及基本路由、防火墙主备配置。

5.3 配置步骤

本节主要介绍IPSec VPN、路由规划、防火墙主备的详细配置

5.1 组网需求

参照2.1.2.1节组网图，营业部跟接入中心间采用双ADSL的链路备份方式，在链路上启用IPSec VPN，加密接入中心跟营业部间数据流的转发，保证数据流的安全可靠。在接入中心内部，防火墙采用主备方式组网，交换机采用堆叠形式工作。

5.2 配置思路

1. 按照IP规划配置所有设备接口IP地址；
2. 在接入中心的接入路由器上配置GRE OVER IPSec VPN；
3. 在接入中心启用OSPF协议；
4. 配置防火墙的主备功能，开启交换机堆叠功能；

5.3 配置步骤

5.3.1 配置设备接口IP

1. 配置接口IP

为了运行动态路由协议（OSPF），必须先给设备正常工作的接口配置IP地址。

举例：AR路由器2200_A#1接口配置

```
//AR路由器2200_A#1物理三层接口IP配置
interface GigabitEthernet0/0/
  ip address 172.17.32.200 255.255.255.0
// AR路由器2200_A#1逻辑三层接口IP配置
vlan 3835
#
interface Vlanif3835
 ip address 172.17.35.1 255.255.255.0
#
interface Ethernet6/0/0
 port link-type access
 port default vlan 3835
```

2. 配置防火墙上的安全区域

为了在防火墙上实现逻辑区域隔离，需要配置不同信任区域，控制各个区域之间的报文转发权限。可以根据实际需求配置。

举例：USG2200_A#1区域划分

//usg2200_A#1划分三个信任区域：trust、untrust、dmz；并把接口加入对应的区域

```
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/2
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/0
 add interface GigabitEthernet1/0/0
#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet0/0/1
```

//开启区域之间包转发权限（默认全部打开，可根据需要调整）

```
firewall packet-filter default permit all
```

5.3.2 接入中心IPSec VPN配置

1. 配置策略模板方式的IPSec

为了方便多个营业部跟接入中心建立IPSec VPN，我们在接入中心采用策略模板方式建立IPSec。这样只要建立一个模板，就可以跟所有的营业部建立IPSec VPN。

举例：AR路由器2200_A#1配置基于策略模板的IPSec VPN

//AR路由器2200_A#1配置IPSec 模板

```
ipsec proposal branch
#
ike peer branch#1 v2
 pre-shared-key cipher %$%$V%`qSF~\9<z[CpV%$Ba-,.2n%$%$
#
ipsec policy-template use 10
 ike-peer branch#1
 proposal branch
#
```

```
ipsec policy branch 10 isakmp template use
//策略模板运用在 wan 口
interface GigabitEthernet0/0/1
 ip address 172.17.32.200 255.255.255.0
 ipsec policy branch
//配置静态路由
ip route-static 10.10.10.5 255.255.255.255 172.17.32.100
```

5.3.3 接入中心路由规划配置

1. 把整个接入中心划分为一个ospf自治区域，接入路由器作为ABR。

为了减少营业部路由器上的路由条目，把每个营业部规划为一个stub区域，区域中心的接入路由器作为ABR。

举例：AR路由器2200_A#1配置OSPF

```
//AR路由器2200_A#1配置OSPF
ospf 100
 area 0.0.0.0
  network 172.17.35.0 0.0.0.255
  network 172.17.36.0 0.0.0.255
 area 0.0.0.100
  network 192.168.1.0 0.0.0.255
  stub no-summary
```

5.3.4 防火墙主备配置

1. 配置防火墙作为主备方式工作。

为了保证接入中心内部的高可靠，防火墙规划为主备工作模式，交换机通过堆叠线链接。

举例：usg2200_A#1主备配置

```
//usg2200_A#1配置hrp
hrp enable
hrp ospf-cost adjust-enable
hrp interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/0
```

```
 ip address 172.17.41.254 255.255.255.0
 hrp track master
#
interface GigabitEthernet1/0/0
 ip address 172.17.35.254 255.255.255.0
 hrp track master
```

6 附录

6.1U盘开局配置模板

U盘开局标配型模板.rar (此模板中未包含AR大包文件)

6.2桌面云兼容性列表

华为桌面云兼容性列表v1.9_(2013-07

6.3FAQ

1. 如何修改WLAN的SSID密码？

登录eSight，参照下图，在“业务>网络>WLAN管理>资源管理>AC”界面下，左键点击右侧“更多”选项选取“ESS模板”

参照下图，选择需要修改的ESS模板，点击右侧的“ ” 图标

参照下图，输入新的SSID密码后，点击“确定”

2. 如何查看证书状态？

➢ 查看 CA 证书状态

此处 PKI 域（test）需与 AR 中配置的 PKI 域一致。

```
[AR#2]dis pki certificate ca test verbose
CA certificate
  Status : Available
  Version: 3
  Serial Number:
    01
  Signature Algorithm: SHA1WITHRSA
  Issuer:
    O=cczq-h25t6e5zy2..z6oxo6
  Validity
    Not Before: 2003-11-20 20:35:08 GMT
    Not After : 2023-11-15 20:35:08 GMT
  Subject:
    O=cczq-h25t6e5zy2..z6oxo6
  Subject Public Key Info:
    Public Key Algorithm : RSA
    RSA Public Key
          Modulus: ( 2048 bit )
            b11ec8c77f6a5458  598e2a0e0fdaf4d8
            bd01466d89f403f1  e5dcb6f2f62a1867
            269e9fd2bb765b7e  6f23dc3b2c617f59
            8d26282dc993d3ed  19073bbe6423dd34
            d04ee66050ea31f0  6ff74fcecb2c5cc8
            31e5f6d72b6bb6e9  03775b3f6cae325c
            65ce1385206437e5  6497826d8e621bc9
            8a320ad3539ba4fb  0f06f25c7740ab33
            fe93a8599896e7c9  ffd842b2411da22e
            5d800de2ba750b29  aeeff1d7b0be831c
            5695b6011a56e28c  f817265063edf2b2
            f0a6cd5b406212fe  5192c6896e0ce5f1
            4d92b98d3334e348  f14d669055c602c2
            ef691f1d587fab01  b5058d59ac58d4c8
            567cf970ac3ccfba  1eef978df1145a53
            53fa407475ae9905  56ee206b1b0ed991
          Exponent: 0x03
  Key Usage:
            CRL Sign
            Certificate Sign
            Digital Signature
  Basic Constraints: critical
    CA: true

  Associated Pki Realm : test

Total Number: 1
```

➢ 查看local证书状态

此处 PKI 域（test）需与 AR 中配置的 PKI 域一致。

```
[AR#2]dis pki certificate local test verbose
Certificate
  Status : Available
  Version: 3
  Serial Number:
    14 8d
  Signature Algorithm: SHA1WITHRSA
  Issuer:
    O=cczq-h25t6e5zy2..z6oxo6
  Validity
    Not Before: 2013-04-07 07:38:47 GMT
    Not After : 2015-04-08 07:38:47 GMT
  Subject:
    O=cczq-h25t6e5zy2..z6oxo6
    OU=users
    CN=cczq-vpn-01
  Subject Public Key Info:
    Public Key Algorithm : RSA
    RSA Public Key
          Modulus: ( 1024 bit )
            b1c9a3910d79d159  37c1b1945b0d3de1
            ad17c5ceccadf490  92d7d0e6ce775a2a
            334a9da992be3c2a  d469fc600529952a
            107a4df4226e577c  2d79392d0ab91aa2
            9db8a802f298082e  1b6d91fb212146c3
            87bd8164ce351a58  806a38f9ba382b4c
            7302e4389c562022  08b52cbb083eda2e
            ceb8d3b8b46a65d0  10fb31da4705e9c5
          Exponent: 0x010001
  Key Usage:
            Key Encipherment
            Digital Signature
  Basic Constraints:
    CA: false
  CRL Distribution Point:
  URL=http://cczq-h25t6e5zy2:18264/ICA_CRL1.crl

  Associated Pki Realm : test

Total Number: 1
```

3. 上网行为管理如何配置只能查看行情不能进行股票交易策略？

登录ASG，参照下图配置上网管理策略