快速配置

华为S系列园区交换机

文档版本：V1.3（2015-12-10）

HUAWEI TECHNOLOGIES CO., LTD

HUAWEI

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://e.huawei.com/cn

目录

1 开始之前

本文档帮助您首次登录及快速配置华为S系列交换机。更多业务配置，请查阅《交换机配置指南》。

说明

本文适用于交换机V200R003C00及更高版本。

在开始数据配置之前，请您首先完成如下工作：

1. 完成交换机的安装、上电，具体操作请参考《S9700&S7700 快速安装指南》，《S12700 快速安装指南》，《S2700&S3700&S5700&S6700 快速入门》。

2. 如果框式交换机采用集群组网，可参考《 S12700&S9700&S7700 集群安装指导》完成集群线缆连接。

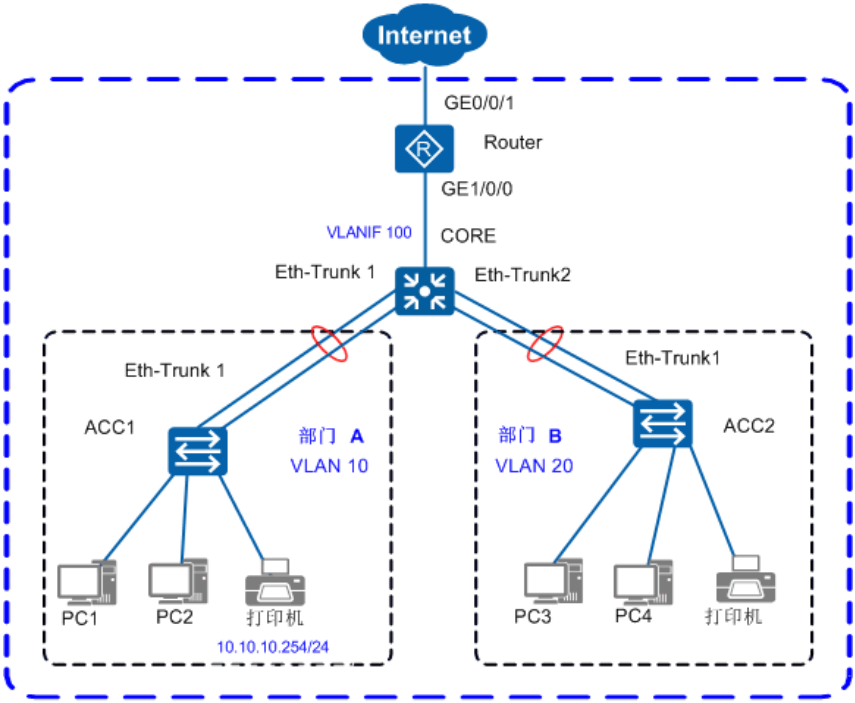
3. 获取以下*常用联系方式*信息，并打印和张贴在您的工作台附近。
   - 华为企业业务技术支持热线电话（400-822-9999）。
   - 负责贵单位网络建设和服务的代理商的联系电话。

4. 访问华为企业技术支持网站（http://support.huawei.com/enterprise）并注册一个*用户账号*，以获取更多的便利，浏览或下载更有价值的产品文档、案例、公告等信息，并可获得订阅和推送方面的支持。

2 小型园区组网场景

说明

本文配置步骤以图中所示的接入交换机*ACC1（S2750）*，核心交换机*CORE（S5700）*和出口路由器*Router（AR系列路由器）*为例。



ACC1	Eth -Trunk1 GE 0/0/ 1 GE 0/0/ 2	PC1/PC2 Eth 0/0/2 Eth 0/0/3	打印机 Eth0/0/4
CORE	Eth -Trunk1 GE 0/0/ 1 GE 0/0/ 2	VLAN 100 GE0/0/20	

- 在小型园区中，S2700&S3700通常部署在网络的接入层，S5700&S6700通常部署在网络的核心，出口路由器一般选用AR系列路由器。
- 接入交换机与核心交换机通过*Eth-Trunk*组网保证可靠性。
- 每个部门业务划分到一个*VLAN*中，部门间的业务在CORE上通过*VLANIF*三层互通。
- 核心交换机作为*DHCP Server*，为园区用户分配IP地址 。
- 接入交换机上配置DHCP Snooping功能，防止内网用户私接小路由器分配IP地址；同时配置IPSG功能，防止内网用户私自更改IP地址。

2.1 数据规划

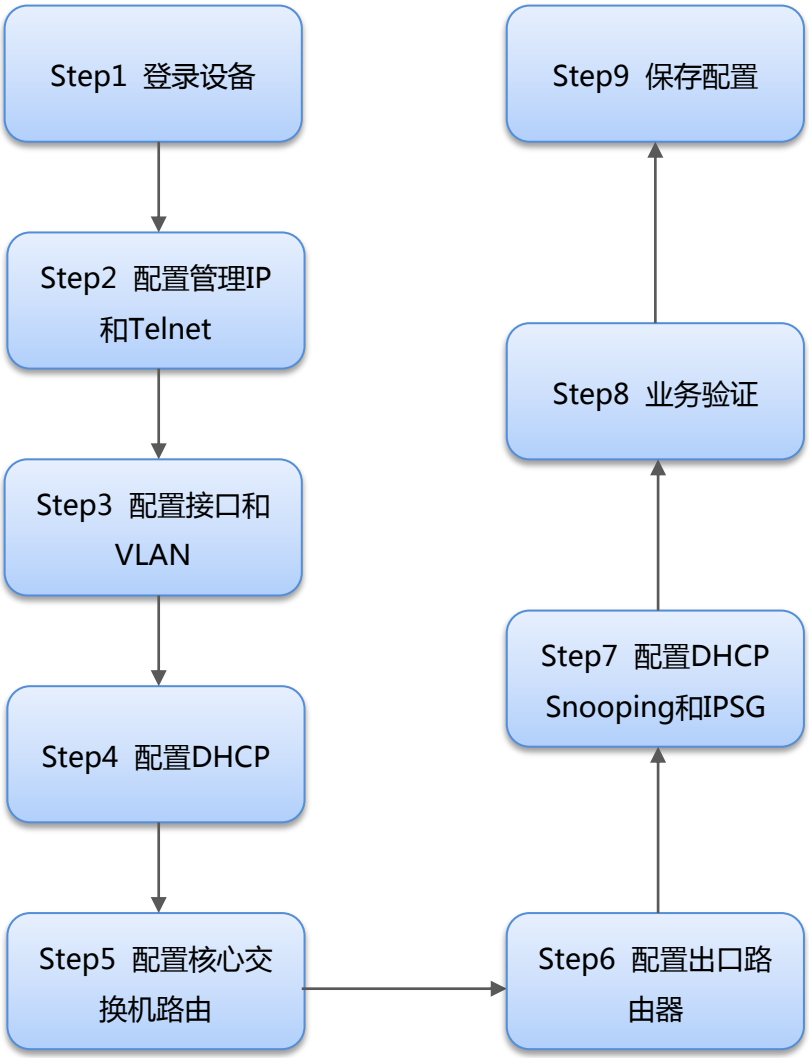
在配置之前，需按照下面的表格准备好数据。以下数据将在本文后续章节使用。

操作	准备项	数据	说明
配置管理IP和Telnet	管理IP地址	10.10.1.1/24	管理IP用于登录交换机。
	管理VLAN	VLAN 5	框式交换机管理口是Ethernet0/0/0。 S2750&S5700&S6700管理口是MEth0/0/1。 S2700/S3700的管理口需要创建VLANIF接口。 建议使用VLANIF接口进行带内管理。
配置接口和VLAN	Eth-Trunk 类型	静态LACP	Eth-Trunk链路有手工负载分担和静态LACP两种工作模式。
	端口类型	连接交换机的端口建议设置为trunk，连接PC的端口设置为access。	trunk 类型端口一般用于连接交换机。 access 类型端口一般用户连接PC。 hybrid类型端口是通用端口，既可以用来连接交换机，也可用来以连接PC。
	VLAN ID	ACC1：VLAN 10 ACC2：VLAN 20 CORE： VLAN 100 、10、20	交换机有缺省VLAN1。 为二层隔离部门A和部门B，将部门A划分到VLAN 10中，部门B划分到VLAN 20中。 CORE通过VLANIF100连接出口路由器。
配置DHCP	DHCP Server	CORE	在园区核心交换机CORE上部署DHCP Server。
	地址池	VLAN 10：ip pool 10 VLAN 20：ip pool 20	部门A的终端从ip pool 10中获取IP地址。 部门B的终端从ip pool 20中获取IP地址。
	地址分配方式	基于全局地址池	无
配置核心交换机路由	IP地址	CORE: VLANIF100 10.10.100.1/24 VLANIF10 10.10.10.1/24 VLANIF20 10.10.20.1/24	VLANIF100是CORE与园区出口路由器对接的IP地址，用于园区内部网络与出口路由器互通。 核心交换机上需要配置一条缺省路由下一跳指向出口路由器。 在CORE上配置VLANIF10、VLANIF20的IP地址后，部门A与部门B之间可以通过CORE互访。

操作	准备项	数据	说明
配置出口路由器	公网接口IP地址	GE0/0/1：202.101.111.2/30	GE0/0/1为出口路由器连接Internet的接口，一般称为公网接口。
	公网网关	202.101.111.1/30	该地址是与出口路由器对接的运营商设备的IP地址，出口路由器上需要配置一条缺省路由指向该地址，用于指导内网流量转发至Internet。
	DNS地址	202.101.111.195	DNS服务器用于将域名解析成 IP地址。
	内网接口IP地址	GE1/0/0：10.10.100.2/24	GE1/0/0为出口路由器连接内网的接口。
配置DHCP Snooping和IPSG	信任接口	Eth-Trunk1	无

2.2 快速配置小型园区

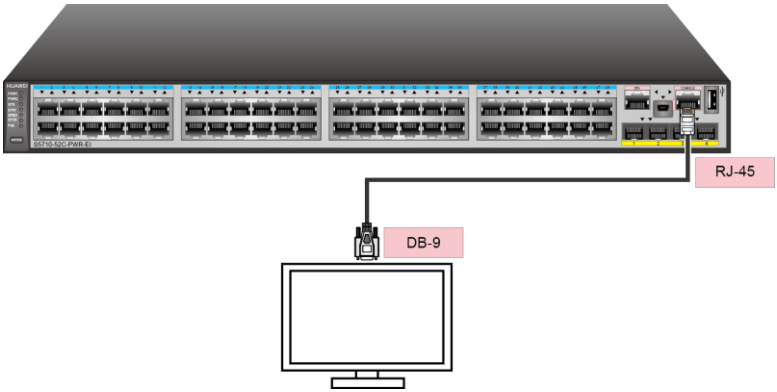
您可以按照下列流程配置各设备的的数据，连通园区内部用户，并使内部用户可访问外网。



登录设备（以交换机为例）

回到组网场景

1 请使用Console通信电缆（产品随设备附带）连接交换机与PC。若PC无串口，需要使用USB接口转串口的转接线。



说明

支持Mini USB接口的设备也可以选择使用Mini USB线缆将交换机连接到PC，详细配置可参见《配置指南-基础配置》。

2 在PC上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。

连接的接口请根据实际情况进行选择。例如，在Windows系统中，可以通过在“设备管理器”中查看端口信息，选择连接的接口。交换机上的通信参数如表1所示。

表1 交换机Console口缺省值

参数	缺省值
传输速率	9600bit/s
流控方式	无
校验方式	无
停止位	1
数据位	8

3 在PC的终端仿真软件界面按**Connect**键，直到出现如下信息，提示用户设置登录密码。

```
Please configure the login password (8-16)
Enter Password:
Confirm Password:
```

密码为字符串形式，区分大小写，长度范围是8～16。输入的密码至少包含两种类型字符，包括大写字母、小写字母、数字及特殊字符。特殊字符不包括“？”和空格。

说明

请牢记初次登录时设置的密码，当用户再次通过Console口登录交换机，需要输入此密码。

完成Console登录密码设置后，用户便可以配置交换机，需要帮助可随时键入“?”。

配置管理IP和Telnet

回到组网场景

配置设备管理IP地址后，可以通过管理IP远程登录设备，下面以交换机CORE为例说明配置管理IP和Telnet的方法。

1 配置管理IP地址。

```
<HUAWEI> system-view
[HUAWEI] vlan 5                                  //创建交换机管理VLAN 5
[HUAWEI-VLAN5] management-vlan
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5                      //创建交换机管理VLAN的VLANIF接口
[HUAWEI-vlanif5] ip address 10.10.1.1 24         //配置VLANIF接口IP地址
[HUAWEI-vlanif5] quit
```

2 配置Telnet。

```
[HUAWEI] telnet server enable      //Telnet出厂时是关闭的，需要打开
[HUAWEI] user-interface vty 0 4    //Telnet常用于设备管理员登录，推荐使用AAA认证
[HUAWEI-ui-vty0-4] protocol inbound telnet
                    // V2R6及之前版本缺省支持telnet协议，但是V2R7及之后版本缺省的
                         是SSH协议，因此使用telnet登录之前，必须要先配置这条命令。
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin password irreversible-cipher Helloworld@6789
       //配置管理员Telnet登录交换机的用户名和密码。用户名不区分大小写，密码区分大小写
[HUAWEI-aaa] local-user admin privilege level 15
                                                 //将管理员的账号权限设置为15（最高）
```

说明

使用Telnet协议存在安全风险，建议使用安全级别更高的STelnet V2登录设备，详细配置可参见《配置指南-基础配置》。

3 在维护终端上Telnet到交换机。出现用户视图的命令行提示符表示登录成功。

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1
                                                 //输入交换机管理IP，并回车
Login authentication

Username:admin                                   //输入用户名和密码
Password:
 Info: The max number of VTY users is 5, and the number
       of current VTY users on line is 1.
       The current login time is 2014-05-06 18:33:18+00:00.
<HUAWEI>                                         //用户视图命令行提示符
```

回到组网场景

a.配置接入层交换机

1 以接入交换机ACC1为例，创建ACC1的业务VLAN 10。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1                                  //修改设备名称为ACC1
[ACC1] vlan batch 10                                   //批量创建VLAN
```

2 配置ACC1连接CORE的Eth-Trunk1，透传部门A的VLAN。

```
[ACC1] interface eth-trunk 1
[ACC1-Eth-Trunk1] port link-type trunk    //配置为trunk模式，用于透传VLAN。
[ACC1-Eth-Trunk1] port trunk allow-pass vlan 10
                                          //配置Eth-Trunk1透传ACC1上的业务VLAN
[ACC1-Eth-Trunk1] mode lacp               //配置Eth-Trunk1为LACP模式
[ACC1-Eth-Trunk1] quit
[ACC1] interface GigabitEthernet 0/0/1    //将成员接口加入Eth-Trunk1
[ACC1-GigabitEthernet0/0/1] eth-Trunk 1
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface GigabitEthernet 0/0/2
[ACC1-GigabitEthernet0/0/2] eth-Trunk 1
[ACC1-GigabitEthernet0/0/2] quit
```

3 配置ACC1连接用户的接口，使用户加入VLAN，并将接口配置成边缘端口。

```
[ACC1] interface Ethernet 0/0/2                        //配置连接PC1的接口
[ACC1-Ethernet0/0/2] port link-type access
[ACC1-Ethernet0/0/2] port default vlan 10
[ACC1-Ethernet0/0/2] stp edged-port enable
[ACC1-Ethernet0/0/2] quit
[ACC1] interface Ethernet 0/0/3                        //配置连接PC2的接口
[ACC1-Ethernet0/0/3] port link-type access
[ACC1-Ethernet0/0/3] port default vlan 10
[ACC1-Ethernet0/0/3] stp edged-port enable
[ACC1-Ethernet0/0/3] quit
[ACC1] interface Ethernet 0/0/4                        //配置连接打印机的接口
[ACC1-Ethernet0/0/4] port link-type access
[ACC1-Ethernet0/0/4] port default vlan 10
[ACC1-Ethernet0/0/4] stp edged-port enable
[ACC1-Ethernet0/0/4] quit
```

说明

如果把ACC1下接入的用户都加入VLAN 10，为了配置简单，也可以ACC1上不配置VLAN，而是把CORE的Eth-Trunk1以access方式加入VLAN10，这样Eth-Trunk1接入的用户全部属于VLAN10。

4 配置BPDU保护功能，加强网络的稳定性。

```
[ACC1] stp bpdu-protection
```

b.配置核心层交换机

1 批量创建CORE与ACC1、ACC2以及园区出口路由器互通的VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname CORE                                    //修改设备名称为CORE
[CORE] vlan batch 10 20 100                              //批量创建VLAN
```

2 配置下行接口和VLANIF接口，VLANIF接口用于部门A与部门B之间互访。以CORE连接ACC1的Eth-Trunk1为例。

```
[CORE] interface eth-trunk 1
[CORE-Eth-Trunk1] port link-type trunk    //配置为trunk模式，用于透传VLAN
[CORE-Eth-Trunk1] port trunk allow-pass vlan 10
                                          //配置Eth-Trunk1透传ACC1上的业务VLAN
[CORE-Eth-Trunk1] mode lacp               //配置为LACP模式
[CORE-Eth-Trunk1] quit
[CORE] interface GigabitEthernet 0/0/1    //将成员接口加入Eth-Trunk1
[CORE-GigabitEthernet0/0/1] eth-Trunk 1
[CORE-GigabitEthernet0/0/1] quit
[CORE] interface GigabitEthernet 0/0/2
[CORE-GigabitEthernet0/0/2] eth-Trunk 1
[CORE-GigabitEthernet0/0/2] quit
[CORE] interface Vlanif 10              //配置VLANIF，使部门A与部门B之间三层互通
[CORE-Vlanif10] ip address 10.10.10.1 24
[CORE-Vlanif10] quit
[CORE] interface Vlanif 20              //配置VLANIF，使部门B与部门A之间三层互通
[CORE-Vlanif20] ip address 10.10.20.1 24
[CORE-Vlanif20] quit
```

3 配置上行接口和VLANIF接口，使园区网络与Internet互通。

```
[CORE] interface GigabitEthernet 0/0/20
[CORE-GigabitEthernet0/0/20] port link-type trunk      //配置为trunk模式
[CORE-GigabitEthernet0/0/20] port trunk allow-pass vlan 100 //配置透传VLAN为
                                                    CORE与上行设备的互联VLAN
[CORE-GigabitEthernet0/0/20] quit
[CORE] interface Vlanif 100             //配置VLANIF，使CORE与路由器之间三层互通
[CORE-Vlanif100] ip address 10.10.100.1 24
[CORE-Vlanif100] quit
```

4 完成接口和VLAN的配置后，可以通过以下命令查看配置结果，显示信息说明可查阅《命令参考》。

执行***display eth-trunk*** 命令检查ACC1上的Eth-Trunk接口配置结果。

```
[ACC1] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: LACP
Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-DA
System Priority: 32768      System ID: 0200-0000-6704
Least Active-linknumber: 1  Max Active-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
ActorPortName           Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/1    Selected 100M     32768   2      289     10111100  1
GigabitEthernet0/0/2    Selected 100M     32768   3      289     10100010  1

Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri   SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/1    32768    0012-3321-2212  32768   2      289     10111100
GigabitEthernet0/0/2    32768    0012-3321-2212  32768   3      289     10111100
```

可以看到，ACC1上， 接口GE0/0/1和GE0/0/2 加入了Eth-Trunk 1。

执行***display vlan***命令检查ACC1上的VLAN配置结果。

可以看到，ACC1上，接口Eth0/0/2~Eth0/0/4以Untagged方式加入VLAN10，Eth-Trunk 1以Tagged方式加入VLAN10。

```
[ACC1] display vlan
The total number of VLANs is : 1
--------------------------------------------------------------------------------
U: Up;          D: Down;          TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                 ST: Vlan-stacking;
#: ProtocolTransparent-vlan;      *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
10   common  UT:Eth0/0/2(U)       Eth0/0/3(U)       Eth0/0/4(U)
             TG:Eth-Trunk1(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable  default       enable  disable    VLAN 0010
```

执行***display eth-trunk*** 命令检查CORE上Eth-Trunk接口配置结果。

```
[CORE] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: LACP
Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-DA
System Priority: 32768      System ID: 0200-0000-6703
Least Active-linknumber: 1  Max Active-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
ActorPortName           Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/1    Selected 100M     32768   2      289     10111100  1
GigabitEthernet0/0/2    Selected 100M     32768   3      289     10100010  1

Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri   SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/1    32768    0012-3321-2211  32768   2      289     10111100
GigabitEthernet0/0/2    32768    0012-3321-2211  32768   3      289     10111100
```

可以看到，CORE上， 接口GE0/0/1和GE0/0/2 加入了Eth-Trunk 1。

执行***display vlan***命令检查CORE上VLAN配置结果。

可以看到，CORE上，接口Eth-Trunk1、Eth-Trunk2分别以Tagged方式加入VLAN10和VLAN20；GE0/0/20以Tagged方式加入VLAN100。

```
[CORE] display vlan
The total number of VLANs is : 3
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
10   common  TG:Eth-Trunk1(U)
20   common  TG:Eth-Trunk2(U)
100  common  TG:GE0/0/20(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable  default       enable  disable    VLAN 0010
20   enable  default       enable  disable    VLAN 0020
100  enable  default       enable  disable    VLAN 0100
```

在CORE上配置DHCP Server，使部门A（VLAN10）和部门B （VLAN20）的用户都能获取到正确的IP地址。

以下以部门A为例，说明DHCP Server的配置步骤。

说明

本文以基于全局地址池的DHCP Server举例。还可以配置基于接口地址池的DHCP Server，详细操作请参见《配置指南-IP业务》。

1 创建全局地址池，配置出口网关、租期（采用缺省值1天，不需配置）并配置为打印机（MAC地址为a-b-c）分配固定的IP地址10.10.10.254。

```
<CORE> system-view
[CORE] dhcp enable
[CORE] ip pool 10
[CORE-ip-pool-10] network 10.10.10.0 mask 24      //配置部门A的用户可分配的地址池范围
[CORE-ip-pool-10] gateway-list 10.10.10.1         //配置部门A的用户的网关地址
[CORE-ip-pool-10] static-bind ip-address 10.10.10.254 mac-address a-b-c
                                                  //配置为打印机分配固定的IP地址
[CORE-ip-pool-10] quit
```

2 配置部门A的用户从全局地址池获取IP地址。

```
[CORE] interface vlanif 10
[CORE-Vlanif10] dhcp select global        //配置部门A的用户从全局地址池获取IP地址
[CORE-Vlanif10] quit
```

回到组网场景

3 使用display ip pool命令，分别查看全局地址池10的配置和使用信息。

```
[CORE] display ip pool name 10
Pool-name      : 10
  Pool-No         : 0
  Lease           : 1 Days 0 Hours 0 Minutes
  Domain-name     : -
  DNS-server0     : -
  NBNS-server0    : -
  Netbios-type    : -
  Position        : Local           Status           : Unlocked
  Gateway-0       : 10.10.10.1
  Network         : 10.10.10.0
  Mask            : 255.255.255.0
  VPN instance    : --
```

查看地址池的配置情况。

```
-------------------------------------------------------------------------------
        Start           End      Total  Used  Idle(Expired)  Conflict  Disable
-------------------------------------------------------------------------------
     10.10.10.1    10.10.10.254   253     4        249(0)          0         0
-------------------------------------------------------------------------------
```

查看地址池的使用情况。

说明

在DHCP服务器配置完成后，需要设置终端电脑网卡为自动获取地址，这样终端才能正常从DHCP服务器获取到地址，正常上网。

说明

配置完动态分配地址之后，刚开电脑获取地址的时间比较长，这是因为对于开启了生成树协议的交换机，每当有电脑接入之后导致生成树重新收敛，所以需要的时间比较长；通过关闭接口的生成树协议或者把连接终端的交换机接口配置为边缘端口即可解决。

下面以ACC1为例，说明配置步骤。

关闭接口的生成树协议

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet 0/0/1] stp disable  //undo stp enable命令也可完成该功能
```

配置连接终端设备的交换机接口为边缘端口

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet 0/0/1] stp edged-port enable
```

根据以上任意一种方法，终端电脑刚开机获取地址速度慢的问题就可以有效解决。

1 在CORE上配置一条到园区出口网关的缺省静态路由，使内网数据可以发到出口路由器。

```
[CORE] ip route-static 0.0.0.0 0 10.10.100.2
```

2 在CORE上使用*display ip routing-table*命令查看IP路由表。

```
[CORE] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------
---
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD  10.10.100.2     Vlanif100
       10.10.10.0/24  Direct  0    0           D   10.10.10.1      Vlanif10
       10.10.10.1/32  Direct  0    0           D   127.0.0.1       Vlanif10
       10.10.20.0/24  Direct  0    0           D   10.10.20.1      Vlanif20
       10.10.20.1/32  Direct  0    0           D   127.0.0.1       Vlanif20
       10.10.100.0/24  Direct  0    0          D   10.10.100.1     Vlanif100
       10.10.100.1/32  Direct  0    0          D   127.0.0.1       Vlanif100
```

能够查看到有一条下一跳地址为10.10.100.2的缺省静态路由，表示静态路由配置完成。

三条直连路由是链路发现自动生成。

说明

在配置出口路由器之前需要准备如下数据：公网IP地址：202.101.111.2/30，公网网关地址：202.101.111.1，DNS地址：202.101.111.195，这些参数在申请宽带的时候由运营商提供，实际网络中请以运营商提供的数据为准。

1 配置出口路由器内网接口和公网接口的IP地址。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/0] ip address 202.101.111.2 30
[Router] interface GigabitEthernet 1/0/0
[Router-GigabitEthernet0/0/1] ip address 10.10.100.2 24
```

2 配置允许上网的acl，将所有允许访问Internet的用户网段写入该acl 。

```
[Router] acl 2000
[Router-acl-basic-2000] rule permit source 10.10.10.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 10.10.20.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 10.10.100.0 0.0.0.255
```

3 在连接公网的接口配置NAT转换实现内网用户访问Internet。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 2000
```

4 配置到内网的明细路由和到公网的静态缺省路由。

```
[Router] ip route-static 10.10.10.0 255.255.255.0 10.10.100.1
[Router] ip route-static 10.10.10.0 255.255.255.0 10.10.100.1
[Router] ip route-static 0.0.0.0 0.0.0.0 202.101.111.1
```

5 配置DNS地址解析功能，DNS服务器地址为运营商给的。

```
[Router] dns resolve
[Router] dns server 202.101.111.195
[Router] dns proxy enable
```

配置DHCP Snooping和IPSG

回到组网场景

配置了DHCP功能之后，部门内用户主机可以自动获取地址。但是为了防止员工在内网私自接一个小路由器并开启DHCP自动分配地址的功能，导致内网合法用户获取到了私接的小路由器分配的地址而不能正常上网，还需要配置DHCP Snooping功能。

以下以部门A为例，说明DHCP Snooping的配置过程。

1 在接入交换机ACC1上开启DHCP Snooping功能。

```
<ACC1> system-view
[ACC1] dhcp enable  //使能DHCP功能
[ACC1] dhcp snooping enable //使能DHCP Snooping功能
```

2 在连接DHCP服务器的接口上使能DHCP Snooping功能，并将此接口配置为信任接口。

```
[ACC1] interface eth-trunk 1
[ACC1-Eth-Trunk1] dhcp snooping enable   //使能DHCP Snooping功能
[ACC1-Eth-Trunk1] dhcp snooping trusted  //配置为信任接口
[ACC1-Eth-Trunk1] quit
```

3 在连接终端的接口上使能DHCP Snooping功能。

```
[ACC1] interface ethernet 0/0/2                  //配置连接PC1的接口
[ACC1-Ethernet0/0/2] dhcp snooping enable
[ACC1-Ethernet0/0/2] quit
[ACC1] interface ethernet 0/0/3                  //配置连接PC2的接口
[ACC1-Ethernet0/0/3] dhcp snooping enable
[ACC1-Ethernet0/0/3] quit
[ACC1] interface ethernet 0/0/4                  //配置连接打印机的接口
[ACC1-Ethernet0/0/4] dhcp snooping enable
[ACC1-Ethernet0/0/4] quit
```

完成上述配置之后，部门A的用户就可以从合法的DHCP服务器获取IP地址，内网私接的小路由器分配地址不会干扰到内网正常用户。

为了防止部门内用户私自更改IP地址后攻击网络，在接入交换机开启DHCP Snooping功能后，还需要开启IP报文检查功能，具体配置以ACC1为例。

4 在接入交换机ACC1上开启VLAN10的IP报文检查功能。功能。

```
[ACC1] vlan 10
[ACC1-vlan10] ip source check user-bind enable //使能IP报文检查功能
[ACC1-vlan10] quit
```

这样ACC1从VLAN10收到报文后会将报文与动态绑定表的表项进行匹配，放行匹配的报文，丢弃不匹配的报文。如果不想对整个VLAN收到的报文进行检查，可以只在连接某个终端的接口上开启IP报文检查功能。

说明

如果网络中采用静态分配IP地址，为防止用户私自修改地址攻击网络，可以配置IP+MAC绑定，配置方法请详见《典型配置举例》中“基础特性典型配置>安全典型配置>IPSG配置”的“配置IPSG防止静态主机私自更改IP地址示例”。

关于交换机防止内网私接小路由器（仿冒DHCP服务器）以及防止用户私自更改IP地址的具体说明及详细配置，请参考《配置指南-安全》中“DHCP Snooping配置>配置DHCP Snooping的基本功能、配置举例”和“IPSG配置>配置IPSG、配置举例”。

业务验证

回到组网场景

1 部门内部选两台PC进行ping测试，验证部门内部二层互通是否正常。

以部门A为例， PC1和PC2是通过ACC1实现二层互通的。如果PC1和PC2之间互ping测试正常则说明二层互通正常。

```
<PC1> ping 10.10.10.100                    //假设PC2通过DHCP自动获取的IP地址为10.10.10.100
PING 10.10.10.100 data bytes, press CTRL_C to break
  Reply from 10.10.10.100 : bytes=56 Sequence=1 ttl=253 time=62 ms
  Reply from 10.10.10.100 : bytes=56 Sequence=2 ttl=253 time=16 ms
  Reply from 10.10.10.100 : bytes=56 Sequence=3 ttl=253 time=62 ms
  Reply from 10.10.10.100 : bytes=56 Sequence=4 ttl=253 time=94 ms
  Reply from 10.10.10.100 : bytes=56 Sequence=5 ttl=253 time=63 ms

--- 10.10.10.100 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
```

能Ping通，说明PC1与PC2之间二层互通正常。

2 从两个部门内各选一台PC进行ping测试，验证部门之间通过VLANIF实现三层互通是否正常。

部门A和部门B之间的用户是通过CORE上的VLANIF实现三层互通的。如果PC1和PC3之间互ping测试正常则说明两个部门之间通过VLANIF实现三层互通正常。ping测试命令与步骤 1 类似 。

3 每个部门各选一台PC进行ping公网地址测试，验证公司内网用户访问Internet是否正常。

以部门A为例，一般可以通过在PC1上ping公网网关地址（即与出口路由器对接的运营商设备的IP地址）来验证是否可以访问Internet，如果ping测试正常则说明内网用户访问Internet正常。ping测试命令与步骤 1 类似 。

保存配置

回到组网场景

通过命令行配置的数据是临时性的。如果不保存，交换机重启后这些配置都会丢失。

如果要使当前配置在交换机重启后仍然有效，需要将当前配置保存为配置文件。

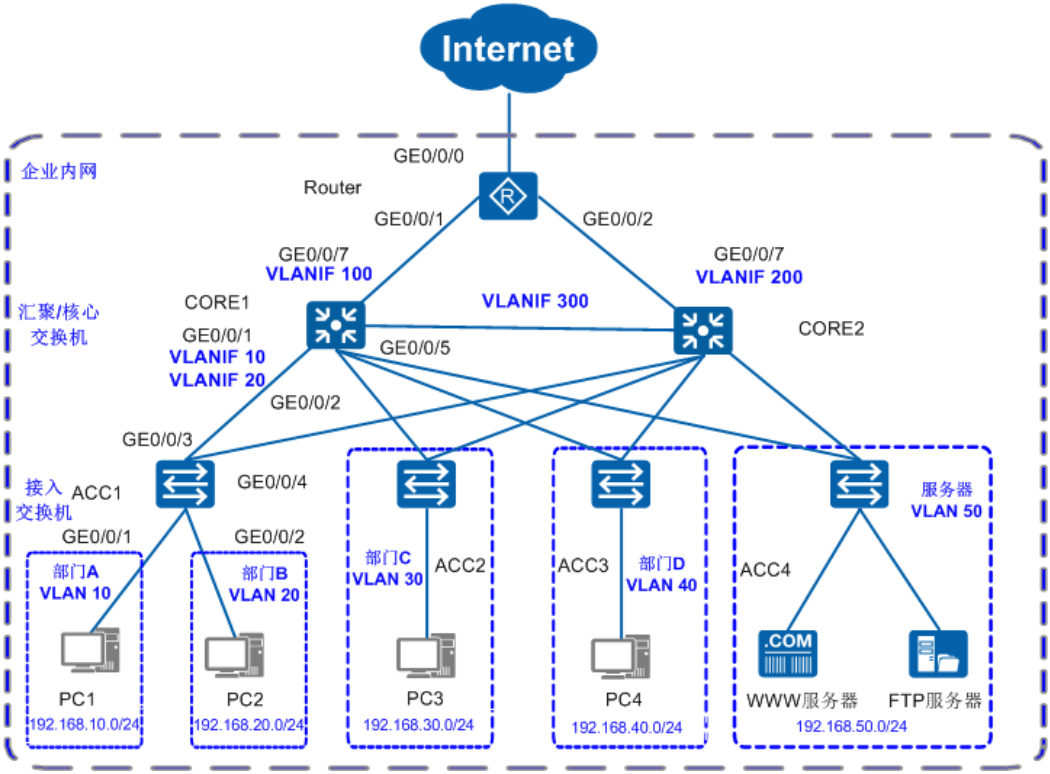
1 保存配置。(以CORE举例)

```
<CORE> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0..
Save the configuration successfully.
```

3 中小园区组网场景

说明

本文配置步骤以图中所示的接入交换机*ACC1（S2750）*，核心交换机*CORE（S5700）*和出口路由器*Router（AR系列路由器）*为例。



- 在中小园区中，S2700&S3700通常部署在网络的接入层，S5700&S6700通常部署在网络的核心，出口路由器一般选用AR系列路由器。
- 核心交换机配置*VRRP*保证网络可靠性，配置*负载分担*有效利用资源。
- 每个部门业务划分到一个*VLAN*中，部门间的业务在CORE上通过*VLANIF*三层互通。
- 核心交换机作为*DHCP Server*，为园区用户分配IP地址。
- 接入交换机上配置*DHCP Snooping*功能，防止内网用户私接小路由器分配IP地址；同时配置*IP报文检查*功能，防止内网用户私自更改IP地址。

3.1 数据规划

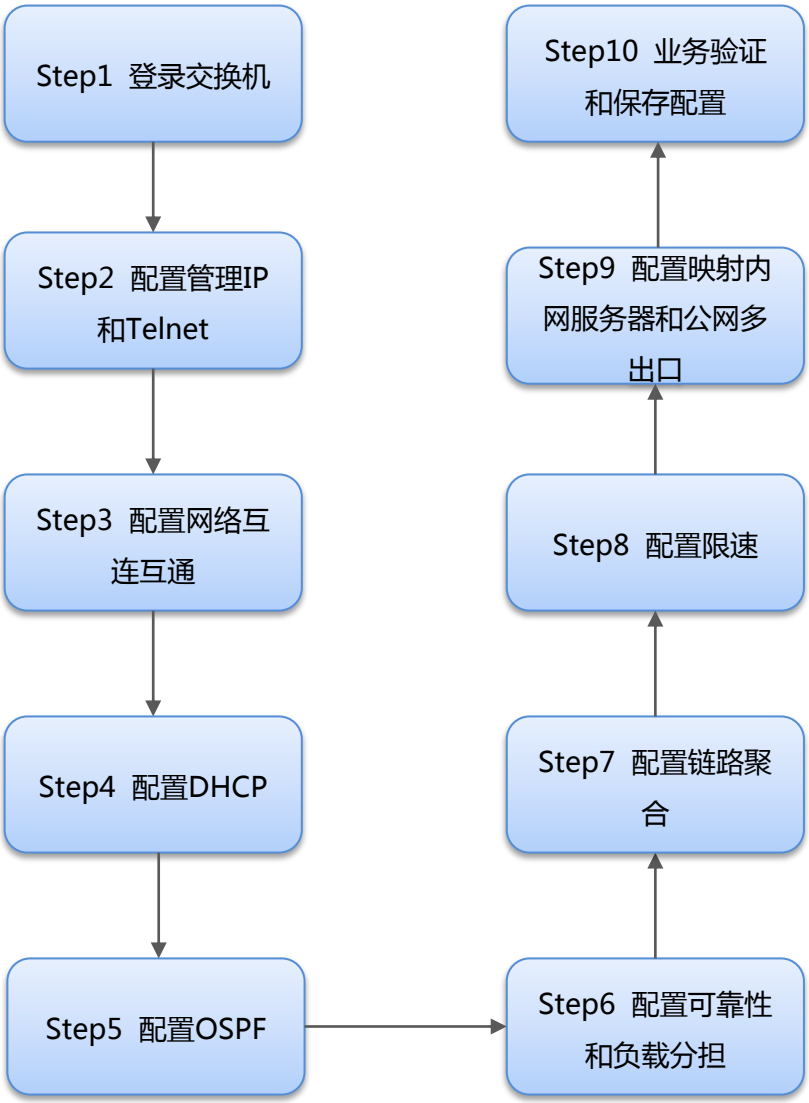
在配置之前，需按照下面的表格准备好数据。以下数据将在本文后续章节使用。

操作	准备项	数据	说明
配置管理IP和Telnet	管理口IP地址	10.10.1.1/24	管理IP用于登录交换机。
	管理VLAN	VLAN 5	框式交换机管理口是Ethernet0/0/0。 S2750&S5700&S6700管理口是MEth0/0/1。 S2700/S3700的管理口需要创建VLANIF接口。 建议使用VLANIF接口进行带内管理。
配置接口和VLAN	端口类型	连接交换机的端口建议设置为trunk，连接PC的端口设置为access。	trunk 类型端口一般用于连接交换机。 access 类型端口一般用户连接PC。 hybrid类型端口是通用端口，既可以用来连接交换机，也可用来以连接PC。
	VLAN ID	ACC1：VLAN 10 20 CORE1： VLAN 10、20、30、40、50、100、300	交换机有缺省VLAN1。 为二层隔离部门A和部门B，将部门A划分到VLAN 10中，部门B划分到VLAN 20中。 CORE1通过VLANIF100连接出口路由器。
配置DHCP	DHCP Server	CORE1、CORE2	在CORE1、CORE2上部署DHCP Server。
	地址池	VLAN 10：ip pool 10 VLAN 20：ip pool 20	部门A的终端从ip pool 10中获取IP地址。 部门B的终端从ip pool 20中获取IP地址。
	地址分配方式	基于全局地址池	无
配置核心交换机	IP地址	CORE1: VLANIF100 172.16.10.1/24 VLANIF300 172.16.30.1/24 VLANIF10 192.168.10.1/24 VLANIF20 192.168.20.1/24	VLANIF100用于CORE1与园区出口路由器对接。VLANIF300用于CORE1与CORE2对接。 CORE1上需要配置一条主用路由，下一跳指向出口路由器；一条备用路由，下一跳指向CORE2。 在CORE1上配置VLANIF10、VLANIF20的IP地址后，部门A与部门B之间可以通过CORE1互访。
	链路聚合	—	Eth-Trunk链路聚合有手工负载分担和静态LACP两种工作模式。

操作	准备项	数据	说明
配置出口路由器	公网接口IP地址	GE0/0/0：202.101.111.2/30	GE0/0/0用于出口路由器连接Internet的接口，一般称为公网接口。
	公网网关	202.101.111.1/30	该地址是与出口路由器对接的运营商设备的IP地址，出口路由器上需要配置一条缺省路由指向该地址，用于指导内网流量转发至Internet。
	DNS地址	202.101.111.195	DNS服务器用于将域名解析成IP地址。
	内网接口IP地址	GE0/0/1：172.16.10.2/24 GE0/0/2：172.16.20.2/24	GE0/0/1、GE0/0/2为出口路由器连接内网的接口，GE0/0/1连接主设备，GE0/0/2连接备设备。
配置DHCP Snooping和IPSG	信任接口	GE0/0/3 GE0/0/4	配置信任接口后，用户只会接收从信任接口进入的DHCP报文，防止内网私接小路由器为主机分配IP地址。
配置内网服务器	FTP服务器 WWW服务器	FTP服务器：192.168.50.10 WWW服务器：192.168.50.20	1、出口路由器会通过NAT实现服务器公网地址和私网地址之间的映射。 2、外网用户可以通过访问公网地址访问服务器。

3.2 快速配置中小园区

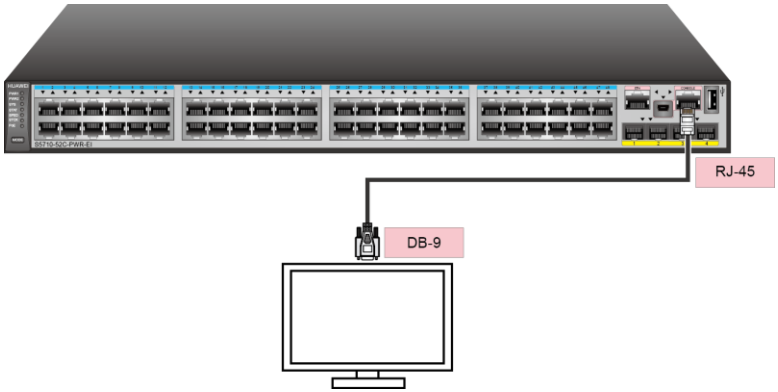
您可以按照下列流程配置各个设备的数据，连通园区内部用户，并使内部用户可访问外网。



登录设备（以交换机为例）

回到组网场景

1 请使用Console通信电缆（产品随机附带）连接交换机与PC。



说明

支持Mini USB接口的设备也可以选择使用Mini USB线缆将交换机连接到PC，详细配置可参见《配置指南-基础配置》。

2 在PC上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。

连接的接口请根据实际情况进行选择。例如，在Windows系统中，可以通过在“设备管理器”中查看端口信息，选择连接的接口。交换机上的通信参数如表1所示。

表1 交换机Console口缺省值

参数	缺省值
传输速率	9600bit/s
流控方式	无
校验方式	无
停止位	1
数据位	8

3 在PC的终端仿真软件界面按**Connect**键，直到出现如下信息，提示用户设置登录密码。

```
Please configure the login password (8-16)
Enter Password:
Confirm Password:
```

密码为字符串形式，区分大小写，长度范围是8～16。输入的密码至少包含两种类型字符，包括大写字母、小写字母、数字及特殊字符。特殊字符不包括“？”和空格。

说明

请牢记初次登录时设置的密码，当用户再次通过Console口登录交换机，需要输入此密码。

完成Console登录密码设置后，用户便可以配置交换机，需要帮助可随时键入“?”。

配置管理IP和Telnet

回到组网场景

配置设备管理IP地址后，可以通过管理IP远程登录设备，下面以交换机CORE1为例说明配置管理IP和Telnet的方法。

1 配置管理IP地址。

```
<HUAWEI> system-view
[HUAWEI] vlan 5                                  //创建交换机管理VLAN 5
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5                      //创建交换机管理VLAN的VLANIF接口
[HUAWEI-vlanif5] ip address 10.10.1.1 24         //配置VLANIF接口IP地址
[HUAWEI-vlanif5] quit
```

2 配置Telnet。

```
[HUAWEI] telnet server enable      //Telnet出厂时是关闭的，需要打开
[HUAWEI] user-interface vty 0 4    //Telnet常用于设备管理员登录，推荐使用AAA认证
[HUAWEI-ui-vty0-4] protocol inbound telnet
                    // V2R6及之前版本缺省支持telnet协议，但是V2R7及之后版本缺省的
                         是SSH协议，因此使用telnet登录之前，必须要先配置这条命令。
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin password irreversible-cipher Helloworld@6789
       //配置管理员Telnet登录交换机的用户名和密码。用户名不区分大小写，密码区分大小写
[HUAWEI-aaa] local-user admin privilege level 15
                                                 //将管理员的账号权限设置为15（最高）
```

说明

使用Telnet协议存在安全风险，建议使用安全级别更高的STelnet V2登录设备，详细配置可参见《配置指南-基础配置》。

3 在维护终端上Telnet到交换机。出现用户视图的命令行提示符表示登录成功。

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1
                                                 //输入交换机管理IP，并回车
Login authentication

Username:admin                                   //输入用户名和密码
Password:
 Info: The max number of VTY users is 5, and the number
       of current VTY users on line is 1.
       The current login time is 2014-05-06 18:33:18+00:00.
<HUAWEI>                                         //用户视图命令行提示符
```

回到组网场景

a.配置接入层交换机

1 以接入交换机ACC1为例，创建ACC1的业务VLAN 10和20。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1                                  //修改设备名称为ACC1
[ACC1] vlan batch 10 20                                //批量创建VLAN
```

2 配置ACC1连接CORE1和CORE2的GE0/0/3和GE0/0/4，透传部门A和部门B的VLAN。

```
[ACC1] interface GigabitEthernet 0/0/3
[ACC1-GigabitEthernet0/0/3] port link-type trunk
                                       //配置为trunk模式，用于透传VLAN。
[ACC1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
                                       //配置GE0/0/3透传ACC1上的业务VLAN
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface GigabitEthernet 0/0/4
[ACC1-GigabitEthernet0/0/4] port link-type trunk
                                       //配置为trunk模式，用于透传VLAN。
[ACC1-GigabitEthernet0/0/4] port trunk allow-pass vlan 10 20
                                       //配置GE0/0/4透传ACC1上的业务VLAN
[ACC1-GigabitEthernet0/0/4] quit
```

3 配置ACC1连接用户的接口，使各部门加入VLAN。

```
[ACC1] interface GigabitEthernet 0/0/1                 //配置连接部门A的接口
[ACC1-GigabitEthernet0/0/1] port link-type access
[ACC1-GigabitEthernet0/0/1] port default vlan 10
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface GigabitEthernet 0/0/2                 //配置连接部门B的接口
[ACC1-GigabitEthernet0/0/2] port link-type access
[ACC1-GigabitEthernet0/0/2] port default vlan 20
[ACC1-GigabitEthernet0/0/2] quit
```

4 配置BPDU保护功能，加强网络的稳定性。

```
[ACC1] stp bpdu-protection
```

说明

如果把ACC1下接入的用户都加入VLAN 10，为了配置简单，也可以ACC1上不配置VLAN，而把CORE1、CORE2与ACC1直接相连的接口以access方式加入VLAN10，这样通过ACC1接入的用户全部属于VLAN10。

b.配置汇聚/核心层交换机

回到组网场景

1 以汇聚/核心交换机CORE1为例，创建其与接入交换机、备份设备以及园区出口路由器互通的VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname CORE1                          //修改设备名称为CORE1
[CORE1] vlan batch 10 20 30 40 50 100 300  //批量创建VLAN
```

2 配置用户侧的接口VLAN和VLANIF，VLANIF接口用于部门之间互访。以CORE1连接ACC1的GE0/0/1接口为例，其他接口不再赘述。

```
[CORE1] interface GigabitEthernet0/0/1
[CORE1-GigabitEthernet0/0/1] port link-type trunk
                                          //配置为trunk模式，用于透传VLAN
[CORE1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 20
                                          //配置GE0/0/1透传ACC1上的业务VLAN
[CORE1-GigabitEthernet0/0/1] quit
[CORE1] interface Vlanif 10                  //配置VLANIF10，使部门之间三层互通
[CORE1-Vlanif10] ip address 192.168.10.1 24
[CORE1-Vlanif10] quit
[CORE1] interface Vlanif 20                  //配置VLANIF20，使部门之间三层互通
[CORE1-Vlanif20] ip address 192.168.20.1 24
[CORE1-Vlanif20] quit
```

3 配置连接出口路由器的接口VLAN和VLANIF。

```
[CORE1] interface GigabitEthernet 0/0/7
[CORE1-GigabitEthernet0/0/7] port link-type trunk      //配置为trunk模式
[CORE1-GigabitEthernet0/0/7] port trunk allow-pass vlan 100
                                  //配置透传VLAN为CORE1与出口路由器的互联VLAN
[CORE1-GigabitEthernet0/0/7] quit
[CORE1] interface Vlanif 100            //配置VLANIF，使CORE1与路由器之间三层互通
[CORE1-Vlanif100] ip address 172.16.10.1 24
[CORE1-Vlanif100] quit
```

4 配置两个核心交换机直连的接口VLAN和VLANIF。

```
[CORE1] interface gigabitethernet 0/0/5
[CORE1-GigabitEthernet0/0/5] port link-type access       //配置为access模式
[CORE1-GigabitEthernet0/0/5] port default vlan 300
[CORE1-GigabitEthernet0/0/5] quit
[CORE1] interface Vlanif 300
[CORE1-Vlanif300] ip address 172.16.30.1 24
[CORE1-Vlanif300] quit
```

c.查看配置结果

回到组网场景

1 完成接口和VLAN的配置后，可以通过以下命令查看配置结果，显示信息说明可查阅《命令参考》。

执行***display vlan***命令检查ACC1上的VLAN配置结果。

可以看到，ACC1上，下行接口已与业务VLAN相对应，上行接口透传所有业务VLAN。

```
[ACC1] display vlan
The total number of VLANs is : 2
--------------------------------------------------------------------------------
U: Up;          D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;                ST: Vlan-stacking;
#: ProtocolTransparent-vlan;     *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type     Ports
--------------------------------------------------------------------------------
10   common   UT: GE0/0/1(U)     TG:GE0/0/3(U)       GE0/0/4(U)
20   common   UT: GE0/0/2(U)     TG:GE0/0/3(U)       GE0/0/4(U)

VID  Status   Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable   default       enable  disable    VLAN 0010
20   enable   default       enable  disable    VLAN 0020
```

2 执行***display vlan***命令检查CORE1上VLAN配置结果。

可以看到，CORE1上，与各接入交换机相连的接口已加入接入交换机对应的业务VLAN。

```
[CORE1] display vlan
The total number of VLANs is : 7
--------------------------------------------------------------------------------
U: Up;          D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;                ST: Vlan-stacking;
#: ProtocolTransparent-vlan;     *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type     Ports
--------------------------------------------------------------------------------
10   common   TG:GE0/0/1(U)
20   common   TG:GE0/0/1(U)
30   common   TG:GE0/0/2(U)
40   common   TG:GE0/0/3(U)
50   common   TG:GE0/0/4(U)
100  common   TG:GE0/0/7(U)
300  common   UT:GE0/0/5(U)

VID  Status   Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable   default       enable  disable    VLAN 0010
20   enable   default       enable  disable    VLAN 0020
30   enable   default       enable  disable    VLAN 0030
40   enable   default       enable  disable    VLAN 0040
50   enable   default       enable  disable    VLAN 0050
100  enable   default       enable  disable    VLAN 0100
300  enable   default       enable  disable    VLAN 0300
```

d.配置出口路由器的接口地址

回到组网场景

1 配置互连内网的接口地址。

```
<HUAWEI> system-view
[HUAWEI] sysname Router                                    //修改设备名称为Router
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] ip address 172.16.10.2 24
                                                           //配置与主设备互连的接口地址
[Router-GigabitEthernet0/0/1] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] ip address 172.16.20.2 24
                                                           //配置与备设备互连的接口地址
[Router-GigabitEthernet0/0/2] quit
```

2 配置连接公网的接口地址。

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] ip address 202.101.111.2 30
                                                           //配置路由器连接公网的接口地址
[Router-GigabitEthernet0/0/0] quit
```

e.（可选）配置静态路由实现网络互通

若配置动态路由，此步骤则不需配置

1 分别在CORE1和CORE2上面分别配置一条缺省静态路由指向出口路由器及其备份路由。

```
[CORE1] ip route-static 0.0.0.0 0.0.0.0 172.16.1.2
                                                  //CORE1指向出口路由器的缺省静态路由
[CORE1] ip route-static 0.0.0.0 0.0.0.0 172.16.3.2 preference 70
                                                  //CORE1指向CORE2的备份静态路由
[CORE2] ip route-static 0.0.0.0 0.0.0.0 172.16.2.2
[CORE2] ip route-static 0.0.0.0 0.0.0.0 172.16.3.1 preference 70
```

2 在出口路由器配置一条缺省静态路由指向运营商。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.101.111.1
```

3 在出口路由器配置到内网的主备路由，主路由下一跳指向CORE1，备路由下一跳指向CORE2 。

```
[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.1.1
[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.2.1 preference
70                                    //配置到达VLAN10网段指向备设备的备路由
[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.1.1
[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.2.1 preference
70                                    //配置到达VLAN20网段指向备设备的备路由
```

f.配置VRRP主备备份实现虚拟网关冗余

回到组网场景

正常情况下内网用户流量都上送到CORE1进行处理，只有当CORE1出故障之后，VRRP备份组切换CORE2为主设备，内网用户流量上送到CORE2。

1 配置示例：在CORE1和CORE2上创建VRRP备份组1和2，配置CORE1的优先级为120，抢占延时为20秒，作为VLAN10和VLAN20的Master设备

```
[CORE1] interface Vlanif 10
[CORE1-Vlanif10] vrrp vrid 1 virtual-ip 192.168.10.3     //配置VLAN 10的虚地址
[CORE1-Vlanif10] vrrp vrid 1 priority 120              //配置CORE1的优先级为120
[CORE1-Vlanif10] vrrp vrid 1 preempt-mode timer delay 20
[CORE1] interface Vlanif 20
[CORE1-Vlanif20] vrrp vrid 2 virtual-ip 192.168.20.3     //配置VLAN 20的虚地址
[CORE1-Vlanif20] vrrp vrid 2 priority 120
[CORE1-Vlanif20] vrrp vrid 2 preempt-mode timer delay 20
```

2 CORE2的优先级为缺省值，作为VLAN10和VLAN20的Backup设备。

```
[CORE2] interface Vlanif 10
[CORE2-Vlanif10] vrrp vrid 1 virtual-ip 192.168.10.3
[CORE2] interface Vlanif 20
[CORE2-Vlanif20] vrrp vrid 2 virtual-ip 192.168.20.3
```

说明

由于CORE1、CORE2和ACC1之间物理成环，实际链路不成环，而X7系列交换机默认是开启stp功能的。为了避免影响CORE1和CORE2之间VRRP主备备份的状态，在此需要关闭接入交换机连接上行链路接口的stp功能，具体配置命令如下：

```
[ACC1] interface GigabitEthernet 0/0/3
[ACC1-GigabitEthernet0/0/3] stp disable      //配置关闭ACC1上行链路接口的stp功能
[ACC1] interface GigabitEthernet 0/0/4
[ACC1-GigabitEthernet0/0/4] stp disable
```

如果确保网络中没有环路的话也可以直接关闭整机的stp功能，配置命令如下：

```
[ACC1] stp disable
Warning: The global STP state will be changed. Continue? [Y/N] y
```

g.配置出口路由器实现内网共享上网

回到组网场景

1 配置允许上网的ACL 。以VLAN 10和20的用户为例：

```
[Router] acl 2000
[Router-acl-basic-2000] rule permit source 192.168.10.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 192.168.20.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 172.16.1.0 0.0.0.255
                                                    //配置允许VLAN 10的用户上网
[Router-acl-basic-2000] rule permit source 172.16.2.0 0.0.0.255
                                                    //配置允许VLAN 20的用户上网
```

2 在连接公网的接口配置NAT转换实现内网上网。

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] nat outbound 2000
```

3 配置DNS地址解析功能，DNS服务器地址为运营商指定。

```
[Router] dns resolve
[Router] dns server 202.101.111.195
[Router] dns proxy enable
```

4 做完上述配置之后，给内网VLAN10的用户配置静态地址，网关设置为192.168.10.3即可以实现上网。

a.配置DHCP服务器

网络管理员为每个终端配置固定的IP地址，当网络规模逐渐增大，为终端手工配置地址变得繁琐和难以管理。为减轻管理负担，管理员决定所有终端用户全部改为自动从DHCP服务器获取地址，除了个别必须固定地址的终端。

配置核心交换机作为DHCP Server，使所有部门的用户都能动态获取到正确的IP地址。以下以CORE1作为主用DHCP Server，以部门A为例，说明DHCP Server的配置步骤。

说明

- 本文以基于全局地址池的DHCP Server举例。还可以配置基于接口地址池的DHCP Server，详细操作请参见《配置指南-IP业务》。
- VRRP组网环境下，为防止主备切换切换而产生IP地址冲突的问题，因此在配置DHCP服务器时，主设备分配地址段的前一半地址，备设备分配地址段的后一半地址。

1 配置CORE1作为主用DHCP服务器，分配地址段的前一半地址。

```
<CORE1> system-view
[CORE1] dhcp enable
[CORE1] ip pool 10
[CORE1-ip-pool-10] gateway-list 192.168.10.3              //配置网关地址
[CORE1-ip-pool-10] network 192.168.10.0 mask 24           //配置可分配的IP地址范围
[CORE1-ip-pool-10] excluded-ip-address 192.168.10.128 192.168.10.254
                                                          //配置排除地址段后一半地址
[CORE1-ip-pool-10] lease day 0 hour 20 minute 0           //配置租期
[CORE1-ip-pool-10] dns-list 202.101.111.195               //配置DNS服务器地址
[CORE1-ip-pool-10] quit
```

回到组网场景

2 配置CORE2作为备用DHCP服务器，分配地址段的后一半地址。

```
<CORE2> system-view
[CORE2] dhcp enable
[CORE2] ip pool 10
[CORE2-ip-pool-10] gateway-list 192.168.10.3
[CORE2-ip-pool-10] network 192.168.10.0 mask 24
[CORE2-ip-pool-10] excluded-ip-address 192.168.10.1 192.168.10.2
[CORE2-ip-pool-10] excluded-ip-address 192.168.10.4 192.168.10.127
[CORE2-ip-pool-10] lease day 0 hour 20 minute 0
[CORE2-ip-pool-10] dns-list 202.101.111.195
[CORE2-ip-pool-10] quit
```

对VLAN20配置DHCP动态分配地址方式同上。

3 配置部门A的用户从全局地址池获取IP地址。

```
[CORE1] interface vlanif 10
[CORE1-Vlanif10] dhcp select global        //配置部门A的用户从全局地址池获取IP地址
[CORE1-Vlanif10] quit
[CORE2] interface vlanif 10
[CORE2-Vlanif10] dhcp select global
[CORE2-Vlanif10] quit
```

4 使用display ip pool命令，查看全局地址池10的配置和使用情况。

```
[CORE1] display ip pool name 10
 Pool-name      : 10
 Pool-No        : 0
 Lease          : 0 Days 20 Hours 0 Minutes
 Domain-name    : -
 DNS-server0    : 202.101.111.195
 NBNS-server0   : -
 Netbios-type   : -
 Position       : Local           Status          : Unlocked
 Gateway-0      : 192.168.10.3
 Network        : 192.168.10.0
 Mask           : 255.255.255.0
 VPN instance   : --

        Start           End      Total  Used  Idle(Expired)  Conflict  Disable
-------------------------------------------------------------------------------
   192.168.10.1  192.168.10.254   253     1        125(0)         0       127
```

查看地址池的配置情况。

查看地址池的使用情况。

说明

在DHCP服务器配置完成后，需要设置终端电脑网卡为自动获取地址，这样终端才能正常从DHCP服务器获取到地址，正常上网。

说明

配置完动态分配地址之后，刚开电脑获取地址的时间比较长，这是因为对于开启了生成树协议的交换机，每当有电脑接入之后导致生成树重新计算收敛，所以需要的时间比较长；通过关闭接口的生成树协议或者把连接终端的交换机接口配置为边缘端口即可解决。

下面以ACC1为例，说明配置步骤。

关闭接口的生成树协议

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1- GigabitEthernet 0/0/1] stp disable  //undo stp enable命令也可完成该功能
```

配置连接终端设备的交换机接口为边缘端口

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1- GigabitEthernet 0/0/1] stp edged-port enable
```

以上两种方法选择一种进行配置，终端电脑刚开机获取地址速度慢的问题就可以有效解决。

b.配置DHCP snooping和IPSG

回到组网场景

配置了DHCP功能之后，部门内用户主机可以自动获取地址。但是为了防止员工在内网私自接一个小路由器并开启DHCP自动分配地址的功能，导致内网合法用户获取到了私接的小路由器分配的地址而不能正常上网，还需要配置DHCP Snooping功能。

以下以部门A为例，说明DHCP Snooping的配置过程。

1 在接入交换机ACC1上开启DHCP Snooping功能。

```
<ACC1> system-view
[ACC1] dhcp enable  //使能DHCP功能
[ACC1] dchp snooping enable //使能DHCP Snooping功能
```

2 在连接终端的接口上使能DHCP Snooping功能。

```
[ACC1] interface GigabitEthernet 0/0/1                    //配置连接部门A的接口
[ACC1-GigabitEthernet 0/0/1] dhcp snooping enable
[ACC1-GigabitEthernet 0/0/1] quit
[ACC1] interface GigabitEthernet 0/0/2                    //配置连接部门B的接口
[ACC1-GigabitEthernet 0/0/2] dhcp snooping enable
[ACC1-GigabitEthernet 0/0/2] quit
```

3 在连接DHCP服务器的接口上使能DHCP Snooping功能，并将此接口配置为信任接口。

```
[ACC1] interface GigabitEthernet 0/0/3                    //配置连接CORE1的接口
[ACC1-GigabitEthernet 0/0/3] dhcp snooping enable         //使能DHCP Snooping功能
[ACC1-GigabitEthernet 0/0/3] dhcp snooping trusted        //配置为信任接口
[ACC1-GigabitEthernet 0/0/3] quit
[ACC1] interface GigabitEthernet 0/0/4                    //配置连接CORE2的接口
[ACC1-GigabitEthernet 0/0/4] dhcp snooping enable
[ACC1-GigabitEthernet 0/0/4] dhcp snooping trusted
[ACC1-GigabitEthernet 0/0/4] quit
```

完成上述配置之后，部门A的用户就可以从合法的DHCP服务器获取IP地址，内网私接的小路由器分配地址不会干扰到内网正常用户。

为了防止部门内用户私自更改IP地址后攻击网络，在接入交换机开启DHCP Snooping功能后，还需要开启IP报文检查功能，具体配置以ACC1为例。

4 在接入交换机ACC1上开启VLAN10的IP报文检查功能。功能。

```
[ACC1] vlan 10
[ACC1-vlan10] ip source check user-bind enable //使能IP报文检查功能
[ACC1-vlan10] quit
```

这样ACC1从VLAN10收到报文后会将报文与动态绑定表的表项进行匹配，放行匹配的报文，丢弃不匹配的报文。如果不想对整个VLAN收到的报文进行检查，可以只在连接某个终端的接口上开启IP报文检查功能。

说明

如果网络中采用静态分配IP地址，为防止用户私自修改地址攻击网络，可以配置IP+MAC绑定，配置方法请详见《典型配置举例》中“基础特性典型配置>安全典型配置>IPSG配置”的“配置IPSG防止静态主机私自更改IP地址示例”。

关于交换机防止内网私接小路由器（仿冒DHCP服务器）以及防止用户私自更改IP地址的具体说明及详细配置，请参考《配置指南-安全》中“DHCP Snooping配置>配置DHCP Snooping的基本功能、配置举例”和“IPSG配置>配置IPSG、配置举例”。

说明

由于内网互联使用的是静态路由，在链路出现故障之后需要管理员手动配置新的静态路由，造成网络长时间中断，影响业务。为了减少这种故障的发生，使用动态路由协议是一种不错的选择。动态路由有自己的算法，在链路出现故障之后动态路由根据自己的算法及时把流量切换到正常的链路，等到故障恢复之后流量又切过来。下面以动态路由协议OSPF为例进行配置：

1 删除两台汇聚/核心交换机的静态路由配置。

```
[CORE1] undo ip route-static all
[CORE2] undo ip route-static all
```

2 删除出口路由器到内网的静态路由，保留到公网的缺省路由。

```
[Router] undo ip route-static 192.168.10.0 24
[Router] undo ip route-static 192.168.20.0 24
```

3 CORE1的OSPF配置。

```
[CORE1] ospf 100 router-id 2.2.2.2
[CORE1-ospf-100] area 0
[CORE1-ospf-100-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[CORE1-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255
[CORE1-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[CORE1-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255
```

4 CORE2的OSPF配置。

```
[CORE2] ospf 100 router-id 3.3.3.3
[CORE2-ospf-100] area 0
[CORE2-ospf-100-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[CORE2-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255
[CORE2-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[CORE2-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255
```

5 出口路由器的OSPF配置，为了连接内网和公网需要配置指向公网的静态缺省路由，在OSPF进程需要引入缺省路由，同时需要配置一条缺省静态路由指向运营商。

```
[Router] ospf 10 router-id 1.1.1.1
[Router-ospf-10] default-route-advertise always
[Router-ospf-10] area 0
[Router-ospf-10-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[Router-ospf-10-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[Router] ip route-static 0.0.0.0 0.0.0.0 202.101.111.1
```

关于交换机OSPF更详细配置说明及具体的配置命令，请参考对应版本产品文档《配置指南-IP单播路由》中“OSPF配置>配置OSPF及配置举例”。

a. 配置VRRP联动接口检测链路

说明

当CORE1到出口路由器的链路出现故障后，流量会通过CORE1到CORE2的互联链路经由CORE2到达出口路由器，此时就增加了互联链路负担，对互联链路的稳定性和带宽负载要求都很高。现网环境中我们往往希望主备设备的上行接口出现故障的时候可以实现主备的快速切换，通过配置VRRP与接口状态联动功能可以实现此快速切换。在VRRP备份组中配置对上行接口进行监听，当监听到接口down了，设备会通过降低优先级来实现主备切换。

VRRP联动接口监视上行链路。

```
[CORE1] interface Vlanif 10
[CORE1-Vlanif10] vrrp vrid 1 track interface GigabitEthernet0/0/7 reduced
100                                    //配置VRRP与上行接口状态联动监视接口功能
[CORE1-Vlanif10] quit
[CORE1] interface Vlanif 20
[CORE1-Vlanif20] vrrp vrid 2 track interface GigabitEthernet0/0/7 reduced
100
[CORE1-Vlanif20] quit
```

b. 配置负载分担

说明

随着业务的增长，经由CORE1的链路带宽占用率太高，但是经过CORE2的链路是闲置的，这样不但可靠性不好而且浪费资源，有效利用左右两边两条链路显得尤为重要。把VRRP主备备份配置为负载分担，一些VLAN以CORE1为主设备，另一些VLAN以CORE2为主设备，不同VLAN的流量被分配到了左右两条链路上，有效的利用现网资源。 此处CORE1继续作为VLAN10的主设备，修改CORE2的优先级使其成为VLAN20的主设备。

1 首先删除CORE1上面VRRP备份组2的优先级和抢占延时配置。

```
[CORE1-Vlanif20] undo vrrp vrid 2 preempt-mode timer delay
[CORE1-Vlanif20] undo vrrp vrid 2 priority
```

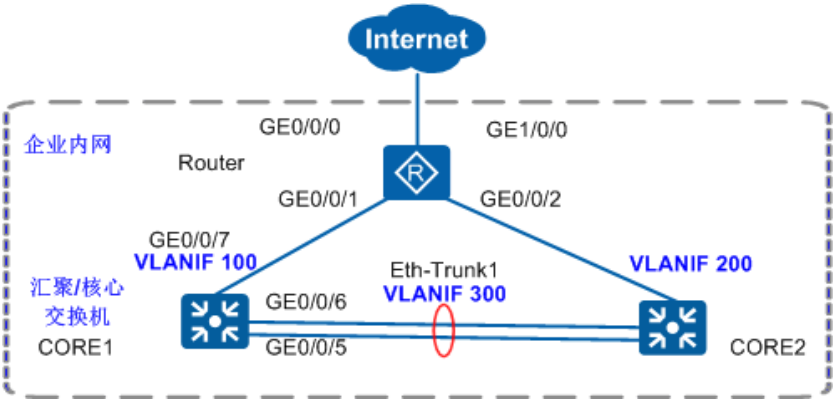
2 配置CORE2为VLAN20的主设备，抢占延时为20S。

```
[CORE2-Vlanif20] vrrp vrid 2 priority 120
[CORE2-Vlanif20] vrrp vrid 2 preempt-mode timer delay 20
```

3 配置VRRP备份组联动上行接口监视上行链路情况。

```
[CORE2-Vlanif20] vrrp vrid 2 track interface GigabitEthernet0/0/7 reduced
100
```

当CORE1或者CORE2的上行发生故障时，流量经过CORE1和CORE2互联的链路，但是单条链路有可能带宽不够，因而造成数据丢失。为了增加带宽，把多条物理链路捆绑为一条逻辑链路，增加带宽的同时提高了链路的可靠性，具体配置如下：



1 恢复接口默认配置（如果接口是默认配置，请直接进行配置即可），将接口恢复为默认配置的步骤和命令如下：

```
[CORE1] interface GigabitEthernet 0/0/5
[CORE1-GigabitEthernet0/0/5] dis this
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 300
#
return
[CORE1-GigabitEthernet0/0/5] undo port default vlan
[CORE1-GigabitEthernet0/0/5] undo port link-type
```

2 V2R5及之后的版本可以用一条命令把接口恢复为初始配置，恢复之后接口被关闭了，需要手动undo shutdown来开启：

```
[CORE1-GigabitEthernet0/0/5] clear configuration this
Warning: All configurations of the interface will be cleared, and its state
will be shutdown. Continue? [Y/N] :y
Info: Total 2 command(s) executed, 2 successful, 0 failed.
[CORE1-GigabitEthernet0/0/5] undo shutdown
```

3 配置链路聚合，配置的步骤和命令如下：

方式一：配置手工负载分担方式的链路聚合

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] trunkport GigabitEthernet 0/0/5 to 0/0/6
[CORE1-Eth-Trunk1] port link-type access
[CORE1-Eth-Trunk1] port default vlan 300
```

方式二：配置LACP模式的链路聚合

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] mode lacp
[CORE1-Eth-Trunk1] trunkport GigabitEthernet 0/0/5 to 0/0/6
[CORE1-Eth-Trunk1] port link-type access
[CORE1-Eth-Trunk1] port default vlan 300
```

在CORE1上配置系统优先级为100，使其成为LACP主动端

```
[CORE1] lacp priority 100
```

在CORE1上配置活动接口上限阈值为2

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] max active-linknumber 2
```

在CORE1上配置接口优先级确定活动链路（配置GE0/0/5和GE0/0/6为活动链路）

```
[CORE1] interface GigabitEthernet 0/0/5
[CORE1-GigabitEthernet0/0/5] lacp priority 100
[CORE1-GigabitEthernet0/0/5] quit
[CORE1] interface GigabitEthernet 0/0/6
[CORE1-GigabitEthernet0/0/6] lacp priority 100
[CORE1-GigabitEthernet0/0/6] quit
```

CORE2的配置同上，只是无需配置系统优先级，使用系统默认的优先级即可。

关于交换机链路聚合的详细说明及具体配置命令，请参考对应版本产品文档：《配置指南-以太网交换》中的“以太网链路聚合配置>配置以太网链路聚合及配置举例”。

a.基于IP地址限速

由于交换机配置每IP限速不是很方便而且需要消耗大量的硬件ACL资源，所以我们只能在AR路由器上配置每IP限速。

由于带宽有限，不能影响正常办公，需要限制内网每个IP地址上传和下载的网速不能超过512kbit/s，在出口路由器连接内网交换机的物理接口做每IP限速。

1 在GE0/0/1接口对192.168.10.0和192.168.20.0的网段做每IP限速，限制为512Kbit/s，配置每IP限速需要注意是在LAN侧接口配置的。因为大多数情况下WAN侧接口做了NAT无法识别内网的IP地址，在LAN侧配置每IP限速时inbound方向对应source地址，限制上传速度，outbound对应destination地址，限制下载速度 。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] qos car inbound source-ip-address range
192.168.10.1 to 192.168.10.254 per-address cir 512
[Router-GigabitEthernet0/0/1] qos car outbound destination-ip-address range
192.168.10.1 to 192.168.10.254 per-address cir 512
[Router-GigabitEthernet0/0/1] qos car inbound source-ip-address range
192.168.20.1 to 192.168.20.254 per-address cir 512
[Router-GigabitEthernet0/0/1] qos car outbound destination-ip-address range
192.168.20.1 to 192.168.20.254 per-address cir 512
```

接口GE0/0/2及其他网段做基于IP限速的方式同上。

b.基于网段总流量限速

随着业务的增长，为了给部门A留有足够的带宽，需要对部门B进行网速限速，要求部门B访问互联网的网速不能超过2M，下载的网速不能超过4M。

1 在出口路由器使用ACL匹配部门B的网段数据流。

```
[Router] acl 2222
[Router-acl-basic-2222] rule permit source 192.168.20.0 0.0.0.255
[Router-acl-basic-2222] quit
```

2 在出口路由器LAN侧接口配置对访问互联网的流量和下载的流量进行限速。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] qos car inbound acl 2222 cir 2048
[Router-GigabitEthernet0/0/1] qos car outbound acl 2222 cir 4096
```

接口GE0/0/2及其他网段做限速的方式同上。

关于AR路由器每IP限速更多的配置说明及详细配置命令，请参考相对应版本产品文档：《配置指南-QoS》中的“流量监管和流量整形配置>配置流量监管>配置举例”。

a.配置映射内网服务器

随着业务的发展，内网的WWW服务器和FTP文件服务器不能仅限于内网用户访问，对外也要提供服务，公网和内网用户都要通过公网地址来访问服务器提供的服务。

1 配置内部服务器，使公网用户通过公网地址访问内网服务器。

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] nat server protocol tcp global current-
interface www inside 192.168.50.99 www
Warning:The port 80 is well-known port. If you continue it may cause
function failure.
Are you sure to continue?[Y/N]:y
[Router-GigabitEthernet0/0/0] nat server protocol tcp global current-
interface ftp inside 192.168.50.199 ftp
```

2 由于FTP是一个多通道协议，需要在出口路由器使能ALG功能。

```
[Router] nat alg ftp enable
```

3 配置内网用户使用公网地址访问内网服务器。

```
[Router] acl 3333
[Router-acl-adv-3333] rule permit ip source 192.168.10.0 0.0.0.255
destination 202.101.111.2 0.0.0.0
[Router-acl-adv-3333] rule permit ip source 192.168.20.0 0.0.0.255
destination 202.101.111.2 0.0.0.0
```

4 在内网接口做NAT转换。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3333
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3333
```

5 分别在内网接口下面做内部服务器映射。

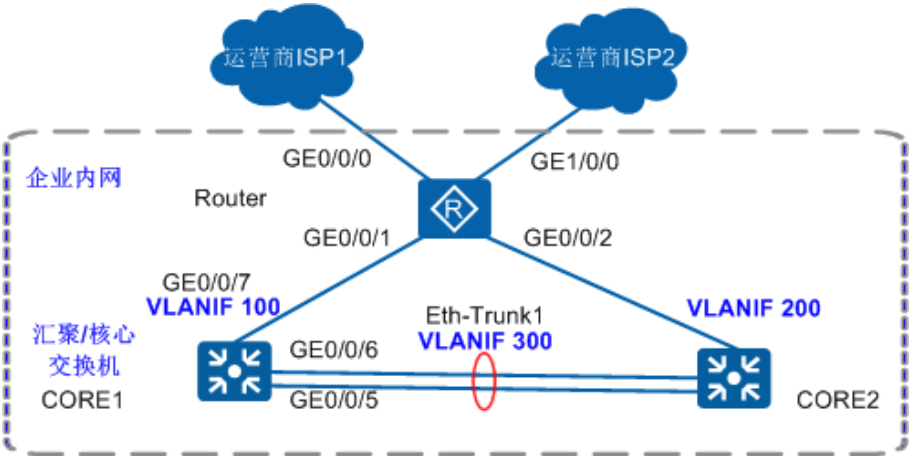
```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat server protocol tcp global interface
GigabitEthernet 0/0/0 www inside 192.168.50.99 www
[Router-GigabitEthernet0/0/1] nat server protocol tcp global interface
GigabitEthernet 0/0/0 ftp inside 192.168.50.199 ftp
```

内网接口GE0/0/2的配置同上。

关于AR路由器配置内网服务器映射的详细说明和具体配置命令，请参考对应版本产品文档：《配置指南-IP业务》中的“NAT配置>配置内部服务器及配置举例”，还可以参考：《典型配置案例》中的”访问Internet外网>NAT“。

b.配置公网多出口

刚开始企业在运营商只申请了一条链路，随着业务的发展，一条链路不能满足企业的网络带宽，需要在原有链路的基础上再申请一条链路，由原来的单出口改为双出口，对内网不同的网段进行控制让其走指定的链路上网。



配置GE1/0/0通过PPPoE拨号上网。

配置策略路由实现不同网段通过不同运营商上网。

1 配置需要进行NAT的ACL。

```
[Router] acl 2015
[Router-acl-basic-2015] rule permit source 192.168.10.0 0.0.0.255
[Router-acl-basic-2015] rule permit source 192.168.20.0 0.0.0.255
```

2 配置拨号访问控制列表。

```
[Router] dialer-rule
[Router-dialer-rule] dialer-rule 1 ip permit
```

3 配置拨号接口。

```
[Router] interface Dialer 0
[Router-Dialer0] ip address ppp-negotiate
[Router-Dialer0] ppp chap user Router
[Router-Dialer0] ppp chap password cipher Router@123
[Router-Dialer0] dialer user user
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] dialer-group 1
[Router-Dialer0] ppp ipcp dns request
[Router-Dialer0] ppp ipcp dns admit-any
```

4 配置使用接口IP地址进行NAT转换。

```
[Router] interface Dialer 0
[Router-Dialer0] nat outbound 2015
```

5 配置TCP最大报文段长度为1200，如果使用默认的1460可能会出现访问网站慢的情况。

```
[Router] interface Dialer 0
[Router-Dialer0] tcp adjust-mss 1200
```

6 在连接运营商线路的物理接口启用PPPoE功能。

```
[Router] interface GigabitEthernet 1/0/0
[Router-GigabitEthernet1/0/0] pppoe-client dial-bundle-number 1
```

7 配置到公网的缺省静态路由，指定出接口为Dialer 0 。

```
[Router] ip route-static 0.0.0.0 0 Dialer 0
```

8 配置ACL匹配数据流，需要把内网互访的数据流不要做重定向。

```
[Router] acl 3000
[Router-acl-adv-3000] rule permit ip source 192.168.10.0 0.0.0.255
destination 192.168.20.0 0.0.0.255
[Router-acl-adv-3000] rule permit ip source 192.168.20.0 0.0.0.255
destination 192.168.10.0 0.0.0.255
[Router-acl-adv-3000] quit
[Router] acl 3001
[Router-acl-adv-3001] rule permit ip source 192.168.10.0 0.0.0.255
[Router-acl-adv-3001] quit
[Router] acl 3002
[Router-acl-adv-3002] rule permit ip source 192.168.20.0 0.0.0.255
[Router-acl-adv-3002] quit
```

9 配置流分类c0、c1和c2，分别匹配ACL3000、ACL3001和ACL3002。 回到组网场景

```
[Router] traffic classifier c0
[Router-classifier-c0] if-match acl 3000
[Router-classifier-c0] quit
[Router] traffic classifier c1
[Router-classifier-c1] if-match acl 3001
[Router-classifier-c1] quit
[Router] traffic classifier c2
[Router-classifier-c2] if-match acl 3002
[Router-classifier-c2] quit
```

10 配置流行为，对内网互访的数据流不做重定向操作，对内网192.168.10.0网段的数据重定向到下一跳202.101.111.1，对内网192.168.20.0网段的数据重定向到出接口Dialer0。

```
[Router] traffic behavior b0
[Router-behavior-b0] permit
[Router-behavior-b0] quit
[Router] traffic behavior b1
[Router-behavior-b1] redirect ip-nexthop 202.101.111.1
[Router-behavior-b1] quit
[Router] traffic behavior b2
[Router-behavior-b2] redirect interface Dialer 0
[Router-behavior-b2] quit
```

11 配置流策略，分别将流分类和流行为组合起来。

```
[Router] traffic policy test
[Router-trafficpolicy-test] classifier c0 behavior b0
[Router-trafficpolicy-test] classifier c1 behavior b1
[Router-trafficpolicy-test] classifier c2 behavior b2
[Router-trafficpolicy-test] quit
```

12 将流策略应用到出口路由器互联内网交换机的接口。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-policy test inbound
[Router-GigabitEthernet0/0/1] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-policy test inbound
[Router-GigabitEthernet0/0/2] quit
```

配置完策略路由之后，内网192.168.10.0网段的数据访问互联网走的是GE0/0/0接口，而192.168.20.0网段的数据访问互联网走的是GE1/0/0接口，通过PPPoE拨号上网。

关于AR路由器策略路由的详细配置说明及具体配置命令，请参考对应版本产品文档：《配置指南-IP单播路由》中的“策略路由配置>配置策略路由>配置接口策略路由”及“配置举例>配置接口策略路由示例”。

回到组网场景

a.业务验证

1 从两个部门内各选一台PC进行ping测试，验证部门之间通过VLANIF实现三层互通是否正常。

以部门A和部门B为例， PC1和PC2是通过CORE1（或CORE2）实现三层互通的。如果PC1和PC2之间互ping测试正常则说明三层互通正常。

```
<PC1> ping 192.168.20.254          //假设PC2通过DHCP自动获取的IP地址为192.168.20.254
 PING 192.168.20.254 data bytes, press CTRL_C to break
    Reply from 192.168.20.254  : bytes=56 Sequence=1 ttl=253 time=62 ms
    Reply from 192.168.20.254 : bytes=56 Sequence=2 ttl=253 time=16 ms
    Reply from 192.168.20.254 : bytes=56 Sequence=3 ttl=253 time=62 ms
    Reply from 192.168.20.254 : bytes=56 Sequence=4 ttl=253 time=94 ms
    Reply from 192.168.20.254 : bytes=56 Sequence=5 ttl=253 time=63 ms

  --- 192.168.20.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

能Ping通，说明PC1与PC2之间三层互通正常。

2 部门内部选两台PC进行ping测试，验证部门内部二层互通是否正常。

部门A的用户是通过ACC1实现二层互通的。如果部门A的用户之间互ping测试正常则说明部门A内二层互通正常。ping测试命令与步骤 1 类似 。

3 每个部门各选一台PC进行ping公网地址测试，验证公司内网用户访问Internet是否正常。

以部门A为例，一般可以通过在PC1上ping公网网关地址（即与出口路由器对接的运营商设备的IP地址）来验证是否可以访问Internet，如果ping测试正常则说明内网用户访问Internet正常。ping测试命令与步骤 1 类似 。

b.保存配置

通过命令行配置的数据是临时性的。如果不保存，交换机重启后这些配置都会丢失。

如果要使当前配置在交换机重启后仍然有效，需要将当前配置保存为配置文件。

以CORE1为例：

```
<CORE1> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0..
Save the configuration successfully.
```

4 常见问题

1 如何清除配置？如何清空配置？如何恢复出厂配置？

说明

恢复出厂配置后，已有配置数据将被全部清除，请提前保存配置文件。

恢复交换机出厂配置。

```
<HUAWEI> reset saved-configuration
Warning: The action will delete the saved configuration in the device.
The configuration will be erased to reconfigure. Continue? [Y/N]:y
Warning: Now clearing the configuration in the device.
Info: Succeeded in clearing the configuration in the device.
<HUAWEI> reboot
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to
the next startup saved-configuration file flash:/vrpcfg.zip. Continue?
[Y/N]:n
Info: If want to reboot with saving diagnostic information, input 'N'
and then execute 'reboot save diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

2 如何一键清除接口配置？

一键清除接口配置，可以执行clear configuration this（接口视图）命令或clear configuration interface （系统视图）命令，并将接口shutdown。

说明

一键清除接口配置后接口被shutdown，需要执行undo shutdown打开接口。

3 如何重置Console密码？

如果用户的Telnet账号具有3级或更高的权限，则可以通过Telnet登录到设备后修改Console密码。

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] authentication-mode password
[HUAWEI-ui-console0] set authentication password cipher huawei@123
[HUAWEI-ui-console0] return
```

4 如何重置Telnet密码？

通过Console口登录交换机，修改Telnet密码。（以AAA验证方式为例）

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user11 password irreversible-cipher huawei@123
```

如果用户不记得原登录的用户名，可以新配置一个用户名和密码，配置方法参见“配置管理IP与Telnet”。

如果Telnet采用Password验证方式，请参考《S7700&S9700 故障处理》中的“密码遗忘”重置Telnet密码。

5 如何配置地址池中不参与自动分配的IP地址？

地址池中的部分IP地址如果需要保留以提供其他的服务，如分配给DNS服务器，需要把这些不参与自动分配的IP地址在地址池中排除出去，防止这些地址被DHCP服务器自动分配出去，引起IP地址冲突。

配置方式：

接口视图下（接口地址池）执行命令：**dhcp server excluded-ip-address** *start-ip-address* [*end-ip-address*]

全局地址池视图下执行命令：**excluded-ip-address** *start-ip-address* [*end-ip-address*]

6 如何配置租期？

缺省情况下，租期为1天。

在咖啡厅、机场、酒店等流动性较大的场所，建议设置较短的租期；在企业办公区域等相对稳定的场所，建议设置较长的租期。

配置方式：

接口视图下（接口地址池）执行命令： **dhcp server lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

全局地址池视图下执行命令： **lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

7 如何为客户端分配固定的IP地址？

有些重要主机为了保证稳定性，需要使用固定的IP地址。

这种情况下，可以为指定客户端分配固定IP地址。被分配的固定IP地址必须在地址池可动态分配的IP地址范围之内。

配置方式：

接口视图下（接口地址池）执行命令： **dhcp server static-bind ip-address** *ip-address* **mac-address** *mac-address*

全局地址池视图下执行命令： **static-bind ip-address** *ip-address* **mac-address** *mac-address* [**option-template** *template-name*]

5 更多的参考资料

在您配置数据的过程中，如果想获得更多的信息，您还可以：

信息	链接
浏览和查阅交换机配置指南	http://support.huawei.com/enterprise/productNewOffering?idAbsPath=7919710|9856733|7923144|7070015&pid=7070015
浏览和查阅交换机典型配置案例集	http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000027299
浏览和查阅交换机配置注意事项集	http://support.huawei.com/ecommunity/bbs/10162193.html?p=1#p10298719
在技术论坛中发帖求助	http://support.huawei.com/ecommunity/bbs/list_4355.html
在知道社区中向专家提问	http://support.huawei.com/ecommunity/ask/list_4355.html
二层交换机与防火墙对接上网	http://support.huawei.com/ecommunity/bbs/10259502.html
三层交换机与防火墙对接上网	http://support.huawei.com/ecommunity/bbs/10259505.html
二层交换机与路由器对接上网	http://support.huawei.com/ecommunity/bbs/10259504.html
三层交换机与路由器对接上网	http://support.huawei.com/ecommunity/bbs/10259506.html
中小型园区/分支出口综合案例	http://support.huawei.com/ecommunity/bbs/10263819.html?p=1#p0
大型园区出口综合案例（防火墙直连）	http://support.huawei.com/ecommunity/bbs/10264472.html
大型园区出口综合案例（防火墙旁路）	http://support.huawei.com/ecommunity/bbs/10265380.html?p=last#p10574748
校园敏捷网络配置综合案例	http://support.huawei.com/ecommunity/bbs/10265972.html