# Project 全部笔记

网络的功能:

1,数据通讯

2,资源共享

3,提高可靠

4,提高系统处理能力

网络历史

60年代,分组交换,可以提高数据传输成功率,降低服务器负担

70~80,TCP/IP

90~至今,web技术

iso 国际标准化组织

ieee 电子与电气工程师学会

WAN 几十公里 internet

LAN 1公里以内 办公室,教室,宿舍

企业级

思科 华为

路由器 交换机

拓扑结构:

1,点对点 , 适用范围是广域网

2,星形,适用范围是局域网,优点是容易扩展,易实现,易于故障排查

3,网状,适用范围是局域网,高可靠

osi七层参考模型(理论框架)

物理层,数据链路层,网络层,传输层,会话层,表示层,应用层

tcp\ip五层模型(实际使用)

物理层,数据链路层,网络层,传输层,应用层

网卡 交换机 路由器 防火墙 PC

PDU协议数据单元:(不同层次数据在传输时用的单位)

物理层--比特流

数据链路层--数据帧

网络层--数据包

传输层--数据段

进入win2008系统

密码:tedu

==========================

运行脚本,教学环境需要:

172.40.50.115

pub目录下找kvm.sh

1,要用root执行(需要添加执行权限)

2,关闭所有虚拟机

成功后看到ok字样

==========================

网络设备命令行视图

1, 用户视图 > system-view

系统视图 ]

接口视图 g0/0/1]

协议视图

quit //返回上一视图

return 或者 快捷键ctrl +z //返回到用户视图

模块 / 子卡/接口号

<Huawei>system-view //进入系统视图

[Huawei]interface GigabitEthernet0/0/1 //进入接口视图

[Huawei-GigabitEthernet0/0/1]quit //返回上一视图

[Huawei]

[Huawei]interface GigabitEthernet0/0/1 //再次进入接口视图

[Huawei-GigabitEthernet0/0/1]return //返回用户视图

<Huawei>

修改主机名

[Huawei]sysname SW1 //在系统视图下将名字修改为SW1

[Huawei]display current-configuration //查看当前配置

[Huawei]display this //查看当前视图配置

[Huawei]display version //查看系统版本,硬件型号等信息

配置用户名和密码:

<Huawei>system-view

[Huawei]aaa //进入aaa认证,此视图支持用户的创建

[Huawei-aaa]local-user admin01 password cipher 123 //创建账户叫admin01,密码123

[Huawei-aaa]quit

[Huawei]user-interface console 0 //进入控制台接口视图

[Huawei-ui-console0]authentication-mode aaa //激活配置

然后使用快捷键 ctrl + ] //退出系统,测试账户密码的配置

<Huawei>save //保存配置,途中按y

<Huawei>reboot //重启,途中按y

ip地址,相当于住址

MAC地址 (硬件地址 物理地址) ,相当于身份证号,全球唯一,不可更改

bit 比特(位) 二进制 0 1

0 1

1+1 10

0123456789 10

0123456789ABCDEF 10

十六进制

52:54:00:35:6e:56

5254:0035:6e56

52-54-00-35-6e-56

1对1 单播通讯

1对多 组播通讯

1对所有 广播通讯

MTU 最大传输单元,通常是1500字节

MAC地址长度48位,前24位记录了厂商标识,后24位记录了产品序号

交换机: 组建局域网的基本设备,可以智能的通过数据帧中的MAC地址

进行数据传递,因此交换机工作在数据链路层.

交换机工作原理

1,学习,学习源mac地址

2,广播,对除了数据来源的所有接口发送广播信息

3,转发,1对1通讯

4,更新,超过300秒无任何数据通讯,交换机会清除对应的mac地址记录

交换机接口设备关机或更换将会立刻删除对应mac地址记录

[Huawei]display mac-address //查看mac地址表

[Huawei]in e0/0/1 //进入e0/0/1接口

[Huawei-ethernet0/0/1]shutdown //关闭接口

[Huawei-ethernet0/0/1]undo shutdown //打开接口

网络功能, 资源共享 ,数据通讯,提高可靠,提高系统处理能力

60,分组交换

70~80 ,tcp/ip

90, web技术

iso

osi

物理层 ,数据链路层,网络层,传输层 应用层

网卡, 交换机, 路由器, 防火墙, PC

比特流, 数据帧 , 数据包, 数据段

拓扑结构

1,点对点 , 广域网

2,星形

3,网状

用户视图,系统视图,接口视图,协议视图 quit

MAC,物理地址,硬件地址

48位 前24位 厂商标识, 后24位厂商赋予的产品序号

交换机的工作原理

学习,广播,转发,更新

广播泛滥

vlan 虚拟局域网

1,控制广播

2,提高安全

3,提高带宽利用

4,降低数据传输延迟

4096个 0~4095 1000+

广播域, 相同广播域中的主机可以接收到来自本域的所有广播

1个广播域=1个部门=1个vlan=相同网段

vlan 2 //创建vlan 2

undo vlan 2 //删除vlan 2

vlan batch 2 6 //创建vlan2和vlan6

vlan batch 2 to 6 //创建vlan2,vlan3,vlan4,vlan5,vlan6

dispaly vlan //查看vlan列表

in e0/0/3 //进入3接口

port link-type access //接口类型修改为access

port default vlan 2 //将此接口加入vlan2

in e0/0/4 //进入4接口

port link-type access //接口类型修改为access

port default vlan 2 //将此接口加入vlan2

或

[Huawei]port-group 1 //进入1号组

[Huawei-port-group-1]group-member Ethernet0/0/3 Ethernet0/0/4 //添加3接口与4接口到该组

[Huawei-port-group-1]port link-type access //对全组接口修改类型

[Huawei-port-group-1]port default vlan 2 //将全组接口加入vlan2

vlan3:

[Huawei]port-group 2 //进入2号组

[Huawei-port-group-2]group-member Ethernet0/0/5 Ethernet0/0/6 //添加5接口与6接口到该组

[Huawei-port-group-2]port link-type access //对全组接口修改类型

[Huawei-port-group-2]port default vlan 3 //将全组接口加入vlan3

最后使用 display vlan 查看配置

SW1

in e0/0/7

port link-type access //接口类型修改为access

port default vlan 3 //将此接口加入vlan3

SW2

in e0/0/7

port link-type access //接口类型修改为access

port default vlan 3 //将此接口加入vlan3

in e0/0/3

port link-type access //接口类型修改为access

port default vlan 3 //将此接口加入vlan3

access 接入链路 承载1个vlan,通常在链接了终端设备(PC)的接口配置

trunk 中继链路 承载多个vlan,通常在两台交换机之间的链路配置

clear configuration interface Ethernet 0/0/7 //在系统视图,清空7接口所有配置,注意清空后接口自动关闭

in e0/0/7 //进入7接口

undo shutdown //开启接口

port link-type trunk //继续在7口中配置中继链路

port trunk allow-pass vlan all //允许所有vlan通过

display this //检查配置

配置思路:

1,规划vlan,需要多少创建多少

2,将对应的接口加入vlan

3,交换机之间的链路配置为trunk

最后pc配置好ip做ping测试

单点故障

链路聚合,提高链路可靠,提高链路带宽

注意:配置之前检查接口是否为默认状态,否则要清空配置

clear configuration interface Ethernet 0/0/7

in e0/0/7

undo shutdown

1,找到要捆绑的接口,至少2个以上

2,创建链路聚合接口

interface Eth-trunk 1 //创建1号链路聚合接口

3,将物理接口加入链路聚合接口

trunkport ethernet 0/0/7 0/0/8 //将7口8口加入并捆绑在一起

port link-type trunk //继续将1号链路聚合口配置为中继链路

port trunk allow-pass vlan all //放行所有vlan

<Hhuawei>undo terminal monitor //在用户视图下关闭某些信息提示

A 1~127 /8

255.0.0.0

B 128~191 /16

255.255.0.0

C 192~223 /24

255.255.255.0

192.168.0.1

172.25.0.10 /24 172.25.0.1~172.25.0.254

255.255.255.0

172.25.0.10 /16 172.25.0.1~172.25.255.254 172.25.0.255 172.25.1.0

255.255.0.0

c类地址可用范围,比如192.168.1.0网段 就是192.168.1.1~192.168.1.254

某网段中 第一个地址是网络ID,最后一个地址是广播地址

172.16.16.16 172.16.0.1~ 172.16.255.254

255.255.0.0

使用路由器链接不同网段

[Huawei]interface GigabitEthernet 0/0/0

[Huawei-GigabitEthernet0/0/1]ip address 192.168.1.254 24

[Huawei-GigabitEthernet0/0/1]quit

[Huawei]interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1]ip address 192.168.2.254 24

网关:终端设备访问其他网段的出口,通常网关由一台三层设备承担,比如路由器

PC1 的ip 192.168.1.1 /24 网关192.168.1.254

PC2 的ip 192.168.2.1 /24 网关192.168.2.254

路由器可以将不同网段的数据进行传递,依靠路由表来选路

路由表指明当前设备可以前往的区域(网段)

路由表中具体可以前往的目的地可以由以下方式获得

1,直连路由 : 在设备接口配置好ip地址并且打开后 自动产生

2,静态路由 : 由管理员手工设置,小规模网络使用

ip route-static 目标网络id 目标网络子网掩码 下一跳地址

R1

[Huawei]ip route-static 192.168.3.0 24 192.168.2.2 //管理员人工指定(增加)该设备可以前往的网段是3.0, 只要将目的地址是3.0的数据扔向2.2即可

[Huawei]ip route-static 192.168.4.0 24 192.168.2.2

R2

[Huawei]ip route-static 192.168.1.0 24 192.168.2.1

三层交换机= 三层路由 + 二层交换

使用三层交换机

可以先关闭信息提示避免干扰

<Huawei>undo terminal monitor

1,创建所需vlan

[Huawei]vlan batch 2 3

2,将接口加入对应vlan

interface g0/0/2

port link-type access

port default vlan 2

interface g0/0/3

port link-type access

port default vlan 3

3,在三层交换机虚拟接口配置ip,作为终端设备的网关

三层交换机配置ip需要在vlan虚拟接口进行

in vlan 1

ip address 192.168.1.254 24

in vlan 2

ip address 192.168.2.254 24

in vlan 3

ip address 192.168.3.254 24

添加普通交换机合理利用三层交换机的接口

1,新添加S3700一台

2,在S3700中创建vlan2 ,vlan3

3,将e0/0/2接口加入vlan2,e0/0/3接口加入vlan3

在两台交换机之间的链路配置trunk并放行所有vlan

S3700

in e0/0/22

port link-type trunk

port trunk allow-pass vlan all

S5700

in g0/0/1

port link-type trunk

port trunk allow-pass vlan all

为S5700的g0/0/2接口赋予ip的方式:

vlan 4 //创建vlan4

in vlan 4 //进入vlan4的虚拟接口

ip address 192.168.4.1 24 //为此接口配ip

in g0/0/2 //进入2口

port link-type access //设置类型

port default vlan 4 //加入vlan4

dis ip interface brief //查看所有配置过的ip

dis vlan //可以在接口后面看到U代表开启D代表关闭

路由 指路

路由设备依靠路由表来传输不同网段数据

1,直连路由,接口配置ip并开启,自动生成

2,静态路由

3,动态路由,是由某些动态路由协议实现,适合大型网络

4,默认路由,是特殊的静态路由,可以访问任意网络

通常配置在末梢网络或网关出口设备

ospf 开放最短路径优先

宣告,告知其他设备自身所连接的网段

S5700:

ospf //进入ospf协议视图

area 0 //进入区域0,小规模网络只需要一个区域,且必须从0开始

network 192.168.1.0 0.0.0.255 //宣告所在网段

network 192.168.2.0 0.0.0.255

network 192.168.3.0 0.0.0.255

network 192.168.4.0 0.0.0.255

路由器:

ospf

area 0

network 192.168.5.0 0.0.0.255

network 192.168.4.0 0.0.0.255

使用默认路由访问外部网段

1,删除路由器5网段的宣告

ospf

area 0

undo network 192.168.5.0 0.0.0.255

2,在三层交换机中配置默认路由(0.0.0.0 0 代表任意网络)

ip route-static 0.0.0.0 0 192.168.4.2

传输层,定义了端口号,实现了端到端的链接

端口总数65536个

范围0~65535

1~1023 知名端口号

TCP 可靠,效率低,面向连接

UDP 不可靠, 效率高,无连接

TCP协议中比较重要的三个标志位

ACK 确认

SYN 打算与对方建立连接

FIN 打算与对方断开链接

三次握手 syn---ack,syn---ack

四次断开 fin---ack---fin---ack

ACL 访问控制列表

高级ACL 3000~3999 源ip 目标ip 源端口 目标端口 协议

基本ACL 2000~2999 源ip

1,创建acl条目

2,在接口应用

255.255.255.0

11111111.11111111.11111111.00000000

192.168.2.100

192.168.2.1 0.0.0.0

0严格匹配

1(8个1就是255) 不匹配

deny 拒绝

permit 允许

使用acl实现禁止192.168.2.1与192.168.1.1通讯

在路由器上配置:

[Huawei]acl 2000 //创建acl2000

[Huawei-acl-basic-2000]rule deny source 192.168.2.1 0 //定义规则,禁止源地址是192.168.2.1的数据通过

[Huawei]interface G0/0/1 //进入1接口

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 2000 //在接口使用acl2000过滤进入的数据

最后验证使用2.1无法与1.1互通,而2.2可以

只允许2.1与1.1通讯,其他主机无法连通1.1

acl 2001 //创建acl2001

[Huawei-acl-basic-2001]rule permit source 192.168.2.1 0 //允许2.1通过

[Huawei-acl-basic-2001]rule deny source any //禁止任何人通过

[Huawei]interface G0/0/1 //进入1接口

[Huawei-GigabitEthernet0/0/1]undo traffic-filter inbound //在接口删除之前启用的acl

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 2001 //在接口应用新的acl

\*注意:acl条目讲究顺序,匹配即立场,上述实验acl的规则不能写反!

display acl 2001 //查看配置的acl

通过高级acl的配置,禁止2.1访问1.1的网站,其他业务不受影响

acl 3000

rule deny tcp source 192.168.2.1 0 destination 192.168.1.1 0 destination-port eq 80

interface G0/0/1 //进入1接口

undo traffic-filter inbound //在接口删除之前启用的acl(如果已经删除了,不用再删除,使用display this验证即可)

traffic-filter inbound acl 3000 //在接口应用新的acl

最后使用2.1访问1.1,效果是能ping通,却访问不了网站

交换机工作在数据链路层, 传输数据帧,可以智能的依靠MAC地址查找目的主机

路由器工作在网络层,传输数据包,依靠路由表完成数据转发

传输层可以实现端到端的数据传递

TCP 高可靠,效率低,面向连接

三次握手,四次断开

UDP 不可靠,效率高,无连接

ACL 基本 2000~2999 对源ip控制 deny permit

高级 3000~3999 对源ip,目的ip,源端口,目的端口,协议

21 ftp tcp

22 ssh tcp

53 dns tcp/udp

80 http tcp

443 https tcp

69 tftp udp

110 pop3 tcp

25 smtp tcp

nat 网络地址转换,可以将内部的私有ip地址与公有ip进行转换

A 1~127

B 128~191

C 192~223

私有ip地址范围

A 10.0.0.0~10.255.255.255

B 172.16.0.0~172.31.255.255

C 192.168.0.0~192.168.255.255

ipv4 42亿

100M 500~800 动态公网ip

100M 50000 静态公网ip www.baidu.com 100.0.0.1

2000

ipv6 海量

配置方式

1,静态nat,一对一转换,一般用在服务器对外网发布服务时使用

2,easy ip,一对多转换,通常对只需要访问外网的设备配置

192.168.0.1 100.0.0.1 > < 100.0.0.2 192.168.0.1

路由器配置

in g0/0/0

ip add 192.168.2.254 24

in g0/0/1

ip add 100.0.0.1 8

进入外网接口配置nat:

nat static global 100.0.0.2 inside 192.168.2.1 //使用静态nat将外部地址100.0.0.2与内部地址192.168.2.1进行一对一绑定

nat static global 100.0.0.3 inside 192.168.2.2

静态nat使用1对1的方式,可以方便的让内外网互访,但成本较高

192.168.2.1 = 100.0.0.2 > < 100.0.0.10

192.168.2.2 = 100.0.0.3 > < 100.0.0.10

easy ip可以让内部多个私有地址通过一个公网ip出门,能最大程度节约公网ip,但如果先在外网向内网发送数据是无法通讯的.

192.168.2.1:2000= 100.0.0.1:2000 > < 100.0.0.10

192.168.2.2:2001 =100.0.0.1:2001 > < 100.0.0.10

使用easy ip让内部主机都通过一个外网的接口ip出门,可以达到节约公网ip的目的

acl 2000

rule permit source any //使用acl定义任何内部地址

进入路由器公网接口

nat outbound 2000 //让内部任何主机都可以利用g0/0/1(外网接口)的ip访问外网

STP 生成树协议,可以避免网络环路产生的广播风暴,达到保护网络的效果,还可以具有备份链路的作用

VRRP 虚拟路由冗余协议

用来实现网关备份,通过虚拟路由器自动分配正真转发数据的节点(某台物理网关设备)

VRRP 成员

1, 主路由器,正在负责数据转发的设备

2, 备份路由器,处于监视状态,主路由器出现故障后立刻被其替代

3, 虚拟路由器,真正充当客户机网关的设备

MS1(左边的S5700)

in vlan 1 //进vlan1接口

ip add 192.168.1.252 24 //配ip

vlan 2 //创建vlan2

in vlan 2 //进vlan2接口

ip add 192.168.2.2 24 //配ip

in g0/0/1 //进接口

port link-type access

port default vlan 2 //加入vlan2

MS2

in vlan 1 //进vlan1接口

ip add 192.168.1.253 24 //配ip

vlan 3 //创建vlan3

in vlan 3 //进vlan3接口

ip add 192.168.3.2 24 //配ip

in g0/0/1 //进接口

port link-type access

port default vlan 3 //加入vlan3

dispaly ip interface brief //查看ip

MS1

ospf

area 0

network 192.168.1.0 0.0.0.255

network 192.168.2.0 0.0.0.255

MS2

ospf

area 0

network 192.168.1.0 0.0.0.255

network 192.168.3.0 0.0.0.255

R(路由器)

ospf

area 0

network 192.168.2.0 0.0.0.255

network 192.168.3.0 0.0.0.255

network 192.168.4.0 0.0.0.255

使用查看路由表命令验证结果

可以只查看含有/24的行

display ip routing-table | include /24

可以临时让1.1使用1.252或者1.253作为网关

可以ping通4.1即可

在两台s5700配置vrrp功能

in vlan 1

vrrp vrid 1 virtual-ip 192.168.1.254 //

配置vrrp功能,组号1,虚拟路由器ip为192.168.1.254

display vrrp brief //查看vrrp状态,两台设备

应该是一主(master)一备(backup)

最后将1.1的网关设置为1.254测试全网互通即可

新增加vlan(部门)

MS1

vlan 10

in vlan 10

ip add 192.168.10.252 24

MS2

vlan 10

in vlan 10

ip add 192.168.10.253 24

将三层交换机与新部门之间的链路配置为trunk

MS1与MS2以及新部门交换机(SW2)相连的接口

in g0/0/3

port link-type trunk

port trunk allow-pass vlan all

SW2

vlan 10

in e0/0/3

port link-type access

port default vlan 10

使用10.1去ping192.168.10.252与10.253都可以通

在 MS1与MS2宣告10网段

ospf

area 0

network 192.168.10.0 0.0.0.255

开启vlan10的vrrp功能

MS1与MS2

in vlan 10

vrrp vrid 10 virtual-ip 192.168.10.254

使用vrrp实现负载均衡

最终需要使MS1成为vlan1的主,MS2成为vlan10的主

MS1

in vlan 1 //进入MS1的vlan1接口

vrrp vrid 1 priority 105 //修改优先级为105,立刻成为vlan1的主

MS2

in vlan 10 //进入MS2的vlan10接口

vrrp vrid 10 priority 105 //修改优先级为105,立刻成为vlan10的主

vlan trunk 链路聚合 stp ospf 静态路由 默认路由 acl vrrp nat

组建大型企业网络

1,规划vlan,每台交换机分别创建vlan10 20 30 40

vlan batch 10 20 30 40

2,将每台主机链接的交换机接口加入所在的vlan

sw1 进入0/0/1接口加入vlan10

in e0/0/1

port link-type access

port default vlan 10

3,将交换机与三层设备链接的链路配置为trunk

sw1~sw3

port-group 1 //创建接口组,为了方便在多个接口实现相同命令

group-member ethernet 0/0/21 ethernet 0/0/22

port link-type trunk

port trunk allow-pass vlan all

sw4

interface eth-trunk 1 //创建链路聚合接口1

trunkport ethernet 0/0/19 0/0/20 //将19和20号口捆一起

port link-type trunk //将聚合接口1配置为trunk

port trunk allow-pass vlan all //允许所有vlan通过

interface eth-trunk 2 //创建链路聚合接口2

trunkport ethernet 0/0/21 0/0/22 //将21和22号口捆一起

port link-type trunk

port trunk allow-pass vlan all

4,添加2台三层交换机,重命名ms1 与 ms2,同时创建之前的4个vlan

sysname ms1

vlan batch 10 20 30 40

port-group 1 //创建接口组,为了方便在多个接口实现相同命令

group-member g0/0/1 to g0/0/3 g0/0/6 //添加了4个口

port link-type trunk //给这个4个口都配成trunk

port trunk allow-pass vlan all

ms1与ms2

interface eth-trunk 1 //创建链路聚合接口1

trunkport gigabitethernet 0/0/4 0/0/5 //将4和5号口捆一起

port link-type trunk

port trunk allow-pass vlan all

5,为三层交换机配置ip,并测试

ms1配置252 , ms2都把252改成253

in vlan 10

ip add 192.168.10.252 24

in vlan 20

ip add 192.168.20.252 24

in vlan 30

ip add 192.168.30.252 24

in vlan 30

ip add 192.168.40.252 24

display ip interface brief //查看所有配置的ip地址

6,配置vrrp实现虚拟网关

ms1成为vlan10与20的主

in vlan 10

vrrp vrid 10 virtual-ip 192.168.10.254

vrrp vrid 10 priority 105 //提高优先级,在vlan10保持主的身份

in vlan 20

vrrp vrid 20 virtual-ip 192.168.20.254

vrrp vrid 20 priority 105 //提高优先级,在vlan20保持主的身份

in vlan 30

vrrp vrid 30 virtual-ip 192.168.30.254

in vlan 40

vrrp vrid 40 virtual-ip 192.168.40.254

ms2成为vlan30与40的主

in vlan 10

vrrp vrid 10 virtual-ip 192.168.10.254

in vlan 20

vrrp vrid 20 virtual-ip 192.168.20.254

in vlan 30

vrrp vrid 30 virtual-ip 192.168.30.254

vrrp vrid 30 priority 105 //提高优先级,在vlan30保持主的身份

in vlan 40

vrrp vrid 40 virtual-ip 192.168.40.254

vrrp vrid 40 priority 105 //提高优先级,在vlan40保持主的身份

排错: 1,首先检查所有ip,子网掩码与网关 , 然后查看所有交换机是否都创建了4个vlan, 所有交换机之间所链接的链路是否全是trunk

7,为三层交换机外网出口配置ip

ms1

vlan batch 50 60

in vlan 50

ip add 192.168.50.2 24

in g0/0/7

port link-type access

port default vlan 50

in vlan 60

ip add 192.168.60.2 24

in g0/0/8

port link-type access

port default vlan 60

ms2

vlan batch 70 80

in vlan 70

ip add 192.168.70.2 24

in g0/0/7

port link-type access

port default vlan 70

in vlan 80

ip add 192.168.80.2 24

in g0/0/8

port link-type access

port default vlan 80

8,同时为路由器配置对应ip

9,为三层交换机开启ospf

ms1

ospf

area 0

network 192.168.10.0 0.0.0.255

network 192.168.20.0 0.0.0.255

network 192.168.30.0 0.0.0.255

network 192.168.40.0 0.0.0.255

network 192.168.50.0 0.0.0.255

network 192.168.60.0 0.0.0.255

ms2

ospf

area 0

network 192.168.10.0 0.0.0.255

network 192.168.20.0 0.0.0.255

network 192.168.30.0 0.0.0.255

network 192.168.40.0 0.0.0.255

network 192.168.70.0 0.0.0.255

network 192.168.80.0 0.0.0.255

R1

ospf

area 0

network 192.168.50.0 0.0.0.255

network 192.168.70.0 0.0.0.255

R2

ospf

area 0

network 192.168.60.0 0.0.0.255

network 192.168.80.0 0.0.0.255

10,添加外部网络,外网设备使用3700交换机

路由器链接外网的接口配置ip

然后配置默认路由

R1与R2

ip route-static 0.0.0.0 0 100.0.0.10 //配置默认路由

ospf

default-route-advertise //对外通告默认路由

11,配置nat让内外互通

R1与R2

acl 2000 //创建acl确定谁可以访问外网的主机

rule permit source any //任何人都可以

in g0/0/2

nat outbound 2000 //进入接口开启nat,列表2000中是所有人