|  |  |  |  |
| --- | --- | --- | --- |
| **核心层** | SW0 | Fa0/1 | 192.168.200.1 |
| Fa0/6 | 192.168.2.2 |
| port-channel 2 | 192.168.50.2 |
| port-channel 3 | 192.168.60.2 |
| SW1 | port-channel 1 | 192.168.40.2 |
| port-channel 2 | 192.168.50.1 |
| SW2 | port-channel 1 | 192.168.40.1 |
| port-channel 3 | 192.168.60.1 |
| Fa0/5 | 192.168.100.2 |
| **防火墙** | ASA0 | Gig1/1 | 192.168.2.1 |
| Gig1/2 | 192.168.1.254 |
| **服务器区** | WEB服务器 |  | 192.168.1.11 Gate:192.168.1.254 |
| 邮件服务器 |  | 192.168.1.22 Gate:192.168.1.254 |
| FTP服务器 |  | 192.168.1.33 Gate:192.168.1.254 |
| **图书馆** | SW3 | vlan10 | 192.168.10.1 |
| vlan20 | 192.168.20.1 |
| Fa0/3 | 192.168.100.1 |
| PC1 |  | 192.168.10.2 Gate:192.168.10.1 |
| PC2 |  | 192.168.10.3 Gate:192.168.10.1 |
| PC3 |  | 192.168.20.2 Gate:192.168.20.1 |
| PC4 |  | 192.168.20.3 Gate:192.168.20.1 |
| **外网** | PC0 |  | 10.1.1.2 Gate:10.1.1.1 |
| R1 | se0/1/0 | 202.204.100.2 |
| Gi0/0 | 10.1.1.1 |
| **出口路由** | R0 | se0/1/0 | 202.204.100.1 |
| Gi0/0 | 192.168.200.2 |

1. 规划 IP 地址及设备端口

（1）路由器端口配置

* 出口路由器R0

int Gi0/0

ip add **192.168.200.2** 255.255.255.0

no shutdown

exit

int Serial0/1/0

ip add **202.204.100.1** 255.255.255.0

clock rate 64000

no shutdown

exit

* 外网路由器R1

int Gi0/0

ip add **10.1.1.1** 255.0.0.0

no shutdown

exit

int Serial0/1/0

ip add **202.204.100.2** 255.255.255.0

clock rate 64000

no shutdown

exit

（2）二层交换机端口配置

* LW0

vlan 10

exit

int range f 0/2-3

switchport mode access

switchport access vlan 10

exit

int f 0/1

switchport mode trunk

switchport trunk allowed vlan all

exit

* LW1

vlan 20

exit

int range f 0/2-3

switchport mode access

switchport access vlan 20

exit

int f 0/1

switchport mode trunk

switchport trunk allowed vlan all

exit

1. 三层交换机端口配置

* SW3

vlan 10

int vlan 10

ip add 192.168.10.1 255.255.255.0

exit

vlan 20

int vlan 20

ip add 192.168.20.1 255.255.255.0

exit

int f 0/3

no switchport

ip address 192.168.100.1 255.255.255.0

no shutdown

exit

* SW0

int f0/1

no switchport

ip address 192.168.200.1 255.255.255.0

no shutdown

exit

int f0/6

no switchport

ip address 192.168.2.2 255.255.255.0

exit

* SW2

int f0/5

no switchport

ip address 192.168.100.2 255.255.255.0

exit

1. 核心层采用两条链路聚合方式增加主干网带宽

show etherchannel summary查看聚合端口配置信息

* SW2

#创建port-channel 1的逻辑接口，进入物理接口f0/3到f0/4的配置模式，设置接口为trunk模式，允许多个VLAN通过，将这些物理接口加入到port-channel 1中，并启用链路聚合。其他port-channel同理。

int port-channel 1

int range f0/3-4

switchport mode trunk

channel-group 1 mode on

int port-channel 3

int range f0/1-2

switchport mode trunk

channel-group 3 mode on

* SW1

int port-channel 1

int range f0/3-4

switchport mode trunk

channel-group 1 mode on

int port-channel 2

int range f0/1-2

switchport mode trunk

channel-group 2 mode on

* SW0

int port-channel 2

int range f0/2-3

switchport mode trunk

channel-group 2 mode on

int port-channel 3

int range f0/4-5

switchport mode trunk

channel-group 3 mode on

1. 运行 OSPF 动态路由协议

查看OSPF 数据库：show ip ospf database

查看OSPF 邻居：show ip ospf neighbor

1. 为三层交换机的聚合端口分配IP

在三个交换机上配置了不同的port-channel接口，并为这些接口分配了IP地址。每个交换机的每个port-channel都被配置为路由模式（而不是交换模式），这意味着它们可以处理IP层的数据，用于实现交换机之间的路由功能或构建高可用性的网络连接。

* SW0

int port-channel 1

no switchport

ip add 192.168.40.1 255.255.255.0

exit

int port-channel 3

no switchport

ip add 192.168.60.1 255.255.255.0

exit

* SW1

int port-channel 1

no switchport

ip add 192.168.40.2 255.255.255.0

exit

int port-channel 2

no switchport

ip add 192.168.50.1 255.255.255.0

exit

* SW2

int port-channel 2

no switchport

ip add 192.168.50.2 255.255.255.0

exit

int port-channel 3

no switchport

ip add 192.168.60.2 255.255.255.0

exit

1. 配置OSPF协议

show ip route 查看路由表

* SW0

router ospf 1

//在OSPF协议中启用路由器接口，并且将该接口连接的所有网络添加到OSPF路由协议中

network 0.0.0.0 255.255.255.255 area 0

exit

//将目的地址为192.168.1.0/24的IP数据包发送到下一跳地址192.168.2.1

ip route 192.168.1.0 255.255.255.0 192.168.2.1

* SW1

router ospf 1

network 0.0.0.0 255.255.255.255 area 0

exit

* SW2

router ospf 1

network 0.0.0.0 255.255.255.255 area 0

exit

* SW3

router ospf 1

network 0.0.0.0 255.255.255.255 area 0

exit

* R0

router ospf 1

network 192.168.200.2 0.0.0.0 area 0

exit

1. 图书馆分为两类用户，一类可通过 NAT 方式访问 Internet，一类禁止访问Internet，仅可访问校内网络

PC 端 ping 外部服务器之后，在 3 分钟内查看地址转换的情况：

show ip nat translations

查看地址转换的统计情况 ：R0#show ip nat statistics

关于连接内网和外网的路由器R0的配置：

1. GigabitEthernet0/0接口作为内部网络，并分配IP地址和启用NAT内部转换。
2. Serial0/1/0接口作为连接外部网络的接口，并分配公网IP地址和启用NAT外部转换。
3. 配置OSPF路由协议，并通告内部网络地址。
4. 设置NAT转换规则，包括动态和静态NAT。
5. 配置默认路由和静态路由。
6. 设置访问控制列表ACL 120来限制特定网段的访问。ACL通常用于过滤网络流量，并允许或拒绝特定的IP地址或IP地址范围访问特定的服务。ACL是按照顺序评估的，一旦找到匹配的规则，就会执行该规则的动作（允许或拒绝），并且不再继续评估后续的规则。

* R0

# 配置GigabitEthernet0/0接口 设置IP地址和子网掩码 标记为NAT内部接口

interface GigabitEthernet0/0

ip address 192.168.200.2 255.255.255.0

ip nat inside

# 配置Serial0/1/0接口，用于连接外部网络 设置公网IP地址和子网掩码 标记为NAT外部接口

interface Serial0/1/0

ip address 202.204.100.1 255.255.255.0

ip nat outside

clock rate 2000000

# 配置OSPF路由协议 记录邻接变化 通告内部网络到OSPF区域0 起源默认路由信息

router ospf 1

log-adjacency-changes

network 192.168.200.2 0.0.0.0 area 0

default-information originate

# NAT转换规则配置，动态NAT基于ACL 120，地址在ACL 120中定义的内部地址将被转换为Serial0/1/0接口的IP地址。overload表示多个内部地址可以映射到同一个外部地址。web服务器和邮件服务器使用静态NAT映射。

ip nat inside source list 120 interface Serial0/1/0 overload

ip nat inside source static 192.168.1.11 202.204.100.11

ip nat inside source static 192.168.1.22 202.204.100.22

#启用无类别路由选择

ip classless

# 路由配置，设置默认和静态路由 未知目的地的数据包发送到下一跳202.204.100.2

ip route 0.0.0.0 0.0.0.0 202.204.100.2

ip route 192.168.1.0 255.255.255.0 192.168.200.1 //---

# 访问控制表ACL配置 拒绝192.168.20.0/24网段访问(vlan20)，允许其他网段访问

access-list 120 deny ip 192.168.20.0 0.0.0.255 any

access-list 120 permit ip 192.168.0.0 0.0.255.255 any

1. 防火墙上只允许 Web 服务器和邮件服务器可以被网络上的其它计算机访问，FTP 服务器只允许内部网络访问
2. 定义了两个网络接口GigabitEthernet1/1和GigabitEthernet1/2，分别命名为out和in，并设置了它们的安全级别和IP地址。
3. 配置了静态路由，使防火墙能够向外部网络发送数据包。
4. 创建了一个扩展访问控制列表（ACL）120，用于控制网络流量。
5. 将访问控制列表应用到防火墙的接口上，以实施访问控制。

* ASA0

# 进入GigabitEthernet1/1接口配置 命名接口为out 设置安全级别为0（通常外部接口安全级别较低）设置接口的IP地址和子网掩码

interface GigabitEthernet1/1

nameif out

security-level 0

ip address 192.168.2.1 255.255.255.0

# 进入GigabitEthernet1/2接口配置

interface GigabitEthernet1/2

nameif in

security-level 100

ip address 192.168.1.254 255.255.255.0

# 配置静态默认路由，指向下一跳IP地址192.168.2.2

route out 0.0.0.0 0.0.0.0 192.168.2.2 1

# 配置访问控制列表120，首先允许内部网络192.168.0.0/16访问ftp服务器192.168.1.33，然后拒绝任何其他地址访问ftp服务器，并允许其他所有IP流量

access-list 120 extended permit ip 192.168.0.0 255.255.0.0 host 192.168.1.33

access-list 120 extended deny ip any host 192.168.1.33

access-list 120 extended permit ip any any

access-list 120 extended permit tcp any any

access-list 120 extended permit icmp any any

access-list 120 extended permit udp any any

# 将访问控制列表120应用于in和out接口的入站和出站方向

access-group 120 in interface in

access-group 120 in interface out

access-group 120 out interface out

access-group 120 out interface in