访问控制列表和NAT

vlan 的配置

sw 0：

Switch(config)#vlan 10

Switch(config-vlan)#name stu

Switch(config-vlan)#exit

Switch(config)#int fa 0/1

Switch(config-if)#sw acc vlan 10

Switch(config-if)#exit

Switch(config)#int fa 0/2

Switch(config-if)#sw mode tr

sw 1：

Switch(config)#vlan 20

Switch(config-vlan)#name tea

Switch(config-vlan)#exit

Switch(config)#int fa 0/1

Switch(config-if)#sw acc vlan 20

Switch(config-if)#exit

Switch(config)#int fa 0/2

Switch(config-if)#sw mode tr

muti sw0：

Switch(config)#vlan 10

Switch(config-vlan)#name stu

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name tea

Switch(config-vlan)#exit

Switch(config)#vlan 30

Switch(config-vlan)#name server

Switch(config-vlan)#exit

Switch(config)#vlan 50

Switch(config-vlan)#name to-internet

Switch(config-vlan)#exit

Switch(config)#int range g 1/0/1-2

Switch(config-if)#sw tr en d

Switch(config-if)#sw mode trunk

Switch(config-if)#exit

Switch(config)#int range g 1/0/3-4

Switch(config-if)#sw acc vlan 30

Switch(config-if)exit

Switch(config)#int g 1/0/5

Switch(config-if)#sw acc vlan 50

Switch(config-if)#exit

三层交换机和路由器的接口ip配置：

muti sw 0：

Switch(config)#int vlan 10

Switch(config-if)#ip add 192.168.1.1 255.255.255.0

Switch(config-if)#exit

Switch(config)#int vlan 20

Switch(config-if)#ip add 192.168.2.1 255.255.255.0

Switch(config-if)#exit

Switch(config)#int vlan 30

Switch(config-if)#ip add 192.168.3.1 255.255.255.0

Switch(config-if)#exit

Switch(config)#int vlan 50

Switch(config-if)#ip add 200.20.20.1 255.255.255.0

Switch(config-if)#exit

注意：cisco三层交换机必须启用三层路由协议，而锐捷交换机不需要

Switch(config)ip routing

router 0：

Router(config)#int g 0/0

Router(config-if)#ip add 200.20.20.3 255.255.255.0

Router(config-if)#no sh

Router(config-if)#exit

Router(config)#int g 0/1

Router(config-if)#ip add 202.120.120.1 255.255.255.0

Router(config-if)#no sh

网络地址转换NAT配置：

Switch(config)#int vlan 10

Switch(config-if)#ip nat inside

Switch(config-if)#exit

Switch(config)#int vlan 20

Switch(config-if)#ip nat inside

Switch(config-if)#exit

Switch(config)#int vlan 30

Switch(config-if)#ip nat inside

Switch(config-if)#exit

Switch(config)#int vlan 50

Switch(config-if)#ip nat outside

Switch(config-if)#exit

Switch(config)#ip nat pool onlyone 200.20.20.2 200.20.20.2 netmask 255.255.255.0

注意：可以一个一个网段写入控制列表，也可以直接写大网段

Switch(config)#access-list 1 permit 192.168.0.0 0.0.255.255

Switch(config)#ip nat inside source list 1 pool onlyone overload

注意：必须添加对外的默认路由，不能启用动态路由协议（在互联网中，私有地址直接过滤掉了）

Switch(config)#ip route 0.0.0.0 0.0.0.0 200.20.20.3

访问控制列表的配置：

muti sw0 ：

Switch(config)#ip access-list extended denystudent

Switch(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 host 192.168.3.3

Switch(config-ext-nacl)#permit ip any any

Switch(config-ext-nacl)#exit

Switch(config)#int vlan 10

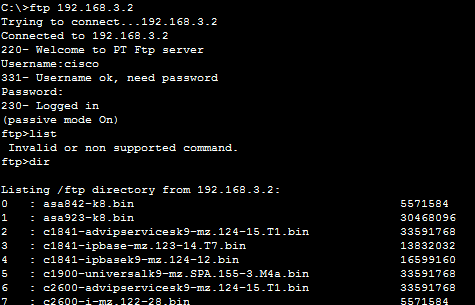
Switch(config-if)#ip access-group denystudent in

Switch(config-if)#exit

题外话：

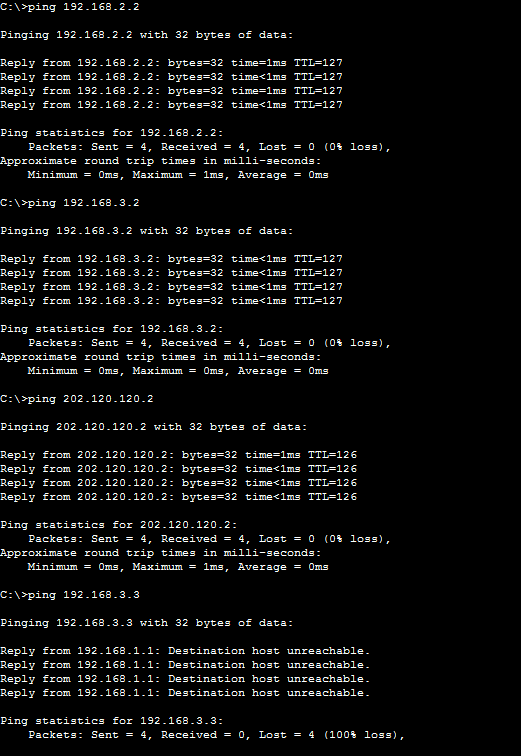
server一般的服务自动配好了的，要访问web服务，使用内部的浏览器，如http://192.168.3.2。

要访问ftp服务，需要注意的是server必须接入到网络中且不能使用浏览器，使用命令行，（用户和口令都是cisco）如：



测试结果：

student主机：



教师机：

