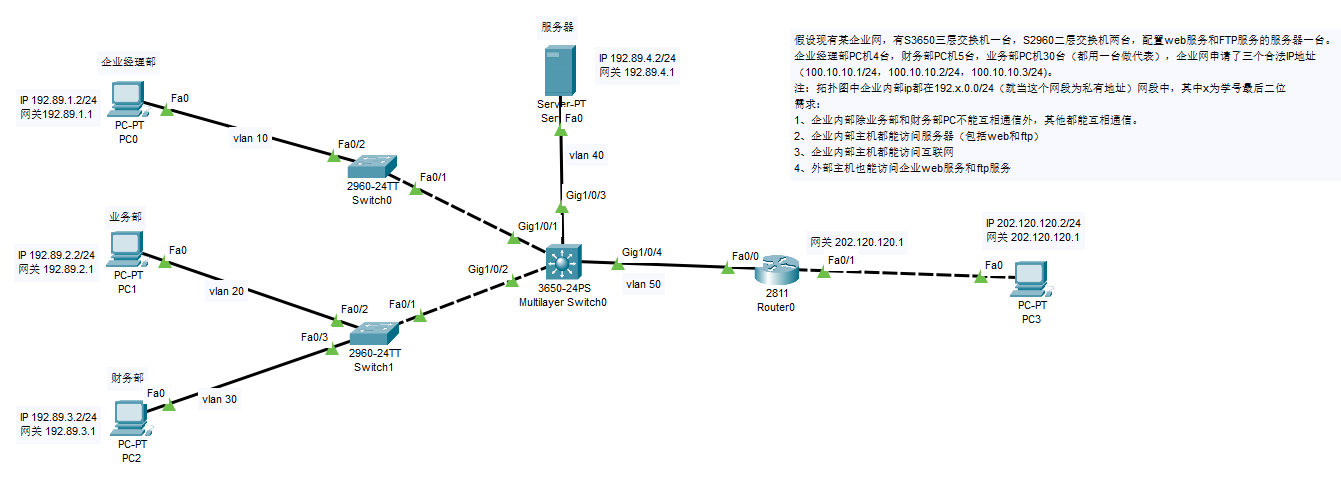
摆好器件无需多言



内网几个 vlan 的配置：

sw 0：

Switch(config)#vlan 10

Switch(config-vlan)#name qiyejinglibu

Switch(config-vlan)#exit

Switch(config)#int fa 0/2

Switch(config-if)#sw acc vlan 10

Switch(config-if)#exit

Switch(config)#int fa 0/1

Switch(config-if)#sw mode tr

sw 1：

Switch(config)#vlan 20

Switch(config-vlan)#name yewubu

Switch(config-vlan)#exit

Switch(config)#vlan 30

Switch(config-vlan)#name caiwubu

Switch(config-vlan)#exit

Switch(config)#int fa 0/2

Switch(config-if)#sw acc vlan 20

Switch(config-if)#exit

Switch(config)#int fa 0/3

Switch(config-if)#sw acc vlan 30

Switch(config-if)#exit

Switch(config)#int fa 0/1

Switch(config-if)#sw mode tr

Multi switch 0：

% Please answer 'yes' or 'no'.

Would you like to enter the initial configuration dialog? [yes/no]:

* No

Switch(config)#vlan 10

Switch(config-vlan)#name qiyejinglibu

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name yewubu

Switch(config-vlan)#exit

Switch(config)#vlan 30

Switch(config-vlan)#name caiwubu

Switch(config-vlan)#exit

Switch(config)#vlan 40

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 g 1/0/3

Switch(config-if)#sw acc vlan 40

Switch(config-if)exit

Switch(config)#int g 1/0/4

Switch(config-if)#sw acc vlan 50

Switch(config-if)#exit

在multi sw0上分配3个部门的vlan 网关

Switch(config)#int vlan 10

Switch(config-if)# ip add 192.89.1.1 255.255.255.0

Switch(config-if)# no sh

Switch(config-if)# exit

Switch(config)#int vlan 20

Switch(config-if)# ip add 192.89.2.1 255.255.255.0

Switch(config-if)# no sh

Switch(config-if)# exit

Switch(config)#int vlan 30

Switch(config-if)# ip add 192.89.3.1 255.255.255.0

Switch(config-if)# no sh

Switch(config-if)# exit

Switch(config)#int vlan 40

Switch(config-if)# ip add 192.89.4.1 255.255.255.0

Switch(config-if)# no sh

Switch(config-if)# exit

Switch(config)#int vlan 50

Switch(config-if)# ip add 100.10.10.1 255.255.255.0

Switch(config-if)# no sh

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

如果不输入这两个指令，将出现主机ping内网的网关都能通，但是这个网关下的主机ip地址通不了的奇葩情况

Switch(config)#ip routing

Switch(config)#do sh ip route

至此内网间都可访问。配置企业经理部电脑：

IP Address 192.89.1.2

Subnet Mask 255.255.255.0

Default Gateway 192.89.1.1

其余依次类推。可发现企业经理部第一次ping 192.89.4.2，第一次丢包后续都能成功

配置外网访问的路由和交换机

router 0：

Router(config)#int fa 0/0

Router(config-if)#ip add 100.10.10.4 255.255.255.0

Router(config-if)#no sh

Router(config-if)#exit

Router(config)#int fa 0/1

Router(config-if)#ip add 202.120.120.1 255.255.255.0

Router(config-if)#no sh

Router(config-if)#exit

Multi-layer switch0:

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 40

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

开放3部门的外网访问：

Switch(config)#ip nat pool shit 100.10.10.2 100.10.10.2 netmask 255.255.255.0

Switch(config)#access-list 1 permit 192.89.1.0 0.0.0.255

Switch(config)#access-list 1 permit 192.89.2.0 0.0.0.255

Switch(config)#access-list 1 permit 192.89.3.0 0.0.0.255

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

Switch(config)#ip route 0.0.0.0 0.0.0.0 100.10.10.4

于是在192.89.3.1上ping 202.120.120.2通

开放外网主机访问内网服务器：

Switch(config)#ip nat inside source static 192.89.4.2 100.10.10.3

于是在202.120.120.2上ping -t 100.10.10.3，第一次丢包后续都能成功

保证业务部不能访问财务部：

muti sw0 ：

Switch(config)#access-list 101 deny ip 192.89.2.0 0.0.0.255 192.89.3.0 0.0.0.255

Switch(config)#access-list 101 permit ip any any

Switch(config)#int vlan 20

Switch(config-if)#ip access-group 101 in

Switch(config-if)#exit

这里一定要用101或者以上的数表明是扩展ACL，不然会报错指令无法识别 蚌

保证财务部不能访问业务部：

Switch(config)#access-list 102 deny ip 192.89.3.0 0.0.0.255 192.89.2.0 0.0.0.255

Switch(config)#access-list 102 permit ip any any

Switch(config)#int vlan 30

Switch(config-if)#ip access-group 102 in

Switch(config-if)#exit

102同理 蚌不住了

最后给出在多层交换机上输入sh run的结果，出了奇怪问题可以比对是否存在指令错误

Switch#sh run

Building configuration...

\*\*\*\*\*\*\*\*\*\*\*\*\*略

interface GigabitEthernet1/0/1

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface GigabitEthernet1/0/2

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface GigabitEthernet1/0/3

switchport access vlan 40

!

interface GigabitEthernet1/0/4

switchport access vlan 50

!

\*\*\*\*\*\*\*\*\*\*\*\*\*略

!

interface Vlan10

mac-address 0030.f23b.db01

ip address 192.89.1.1 255.255.255.0

ip nat inside

!

interface Vlan20

mac-address 0030.f23b.db02

ip address 192.89.2.1 255.255.255.0

ip access-group 101 in

ip nat inside

!

interface Vlan30

mac-address 0030.f23b.db03

ip address 192.89.3.1 255.255.255.0

ip access-group 102 in

ip nat inside

!

interface Vlan40

mac-address 0030.f23b.db04

ip address 192.89.4.1 255.255.255.0

ip nat inside

!

interface Vlan50

mac-address 0030.f23b.db05

ip address 100.10.10.1 255.255.255.0

ip nat outside

!

ip nat pool shit 100.10.10.2 100.10.10.2 netmask 255.255.255.0

ip nat inside source list 1 pool shit overload

ip nat inside source static 192.89.4.2 100.10.10.3

ip classless

ip route 0.0.0.0 0.0.0.0 100.10.10.4

!

ip flow-export version 9

!

!

access-list 1 permit 192.89.1.0 0.0.0.255

access-list 1 permit 192.89.2.0 0.0.0.255

access-list 1 permit 192.89.3.0 0.0.0.255

access-list 101 deny ip 192.89.2.0 0.0.0.255 192.89.3.0 0.0.0.255

access-list 101 permit ip any any

access-list 102 deny ip 192.89.3.0 0.0.0.255 192.89.2.0 0.0.0.255

access-list 102 permit ip any any

!

\*\*\*\*\*\*\*\*\*\*\*\*\*略