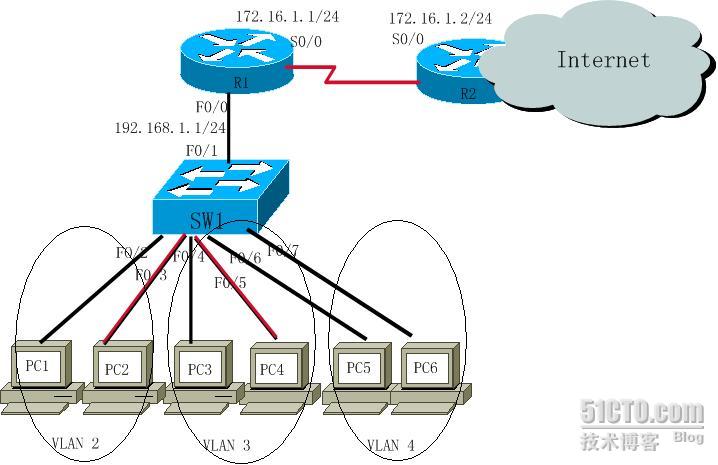
在企业中，要实现所有的员工都能与互联网进行通信，每个人各使用一个公网地址是很不现实的[。](http://www.pcjx.com)一般，企业有1个或几个公网地址，而企业有几十、几百个员工[。](http://www.pcjx.com)要想让所有的员工使用这仅有的几个公网地址与互联网通信该怎么做呢？使用NAT技术！

在企业中，一般会有多个部门，像财务部、技术部、工程部等等[。](http://www.pcjx.com)每个部门有每个部门的职责[。](http://www.pcjx.com)像财务部这种重要的部门有些资料是不允许被其他员工知道的[。](http://www.pcjx.com)怎样能清楚的区分不同的部门，以便于管理呢？使用VLAN技术！

为了工作方便、增强工作效率，各部门经理必须能相互通信[。](http://www.pcjx.com)但不允许员工之间相互通信[。](http://www.pcjx.com)我们又该怎样做呢？使用ACL技术！

今天我们来学习如何使用NAT + VLAN +ACL管理企业网络[。](http://www.pcjx.com)如下是试验环境：



环境介绍：

企业中只有一个公网地址，172.16.1.1/24  
 企业中共有三个部门工程部、财务部、技术部[。](http://www.pcjx.com)  
 PC1 PC3 PC5 分别为三个部门的部门经理使用[。](http://www.pcjx.com)  
 PC1 的ip地址为192.168.1.2/24  
 PC2 的ip地址为192.168.1.3/24  
 PC3 的ip地址为192.168.2.2/24  
 PC4 的ip地址为192.168.2.3/24  
 PC5 的ip地址为192.168.3.2/24  
 PC6 的ip地址为192.168.3.3/24  
 试验目的：  
 通过配置NAT使企业中所有的计算机都能通过唯一的公网地址与互联网通信[。](http://www.pcjx.com)  
 通过配置VLAN划分各个部门，并配置ACL实现每个部门经理之间能够通讯，普通员工之间不能相互通讯[。](http://www.pcjx.com)

OK，知道目的了，让我们开始工作吧！

首先在R1 和 R2上做基本配置，（由于试验过程中要使用VLAN间路由，所以需要使用dot1Q 进行封装来配置子接口）  
 R1  
 Router>en  
 Router#conf t  
 Enter configuration commands, one per line. End with CNTL/Z.  
 Router(config)#host r1  
 r1(config)#int s0/0  
 r1(config-if)#ip addr 172.16.1.1 255.255.255.0  
 r1(config-if)#no shut  
 %LINK-5-CHANGED: Interface Serial0/0, changed state to up  
 r1(config-if)#clock rate 64000  
 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to u  
 r1(config-if)#exit  
 r1(config)#int f0/0  
 r1(config-if)#no ip addr  
 r1(config-if)#no shut  
 r1(config-if)#exit  
 r1(config)#int f0/0.1 配置子接口，  
 r1(config-subif)#encapsulation dot1Q 2 配置子接口必须使用dot1Q进行封装  
 r1(config-subif)#ip addr 192.168.1.1 255.255.255.0  
 r1(config-subif)#no shut  
 r1(config-subif)#exit  
 r1(config)#int f0/0.2 配置子接口  
 r1(config-subif)#encapsulation dot1Q 3 配置子接口必须使用dot1Q进行封装  
 r1(config-subif)#ip addr 192.168.2.1 255.255.255.0  
 r1(config-subif)#no shut  
 r1(config-subif)#exit  
 r1(config)#int f0/0.3 配置子接口  
 r1(config-subif)#encapsulation dot1Q 4 配置子接口必须使用dot1Q进行封装  
 r1(config-subif)#ip addr 192.168.3.1 255.255.255.0

因为我们把R2当作公网使用，所以只需要在R2的S0/0口上配置ip就可以啦  
 R2

Router>en  
 Router#conf t  
 Enter configuration commands, one per line. End with CNTL/Z.  
 Router(config)#host r2  
 r2(config)#int s0/0  
 r2(config-if)#ip addr 172.16.1.2 255.255.255.0  
 r2(config-if)#no shut

基本配置完成了，接下来第一步，我们要让企业中的所有员工都能通过唯一的公网ip 172.16.1.1/24 与互联网相互通信[。](http://www.pcjx.com)  
 R1  
 r1(config)#ip nat pool internet 172.16.1.1 172.16.1.1 netmask 255.255.255.0 定义全局地址池  
 r1(config)#access-list 10 permit 192.168.0.0 0.0.255.255通过标准访问控制列表定义内部网络的上网条件  
 r1(config)#ip nat inside source list 10 pool internet overload 建立全局地址池与标准访问控制列表之间的映射关系  
 r1(config)#int s0/0  
 r1(config-if)#ip nat outside 外网接口绑定（要想配置能实现应用必须在内外网接口上绑定）  
 r1(config-if)#exit  
 r1(config)#int f0/0  
 r1(config-if)#ip nat inside 内网接口绑定

通过配置VLAN划分各个部门，并配置ACL以实现每个部门经理之间能够通讯，普通员工之间不能相互通讯[。](http://www.pcjx.com)

Sw

Switch>en  
 Switch#conf t  
 Enter configuration commands, one per line. End with CNTL/Z.  
 Switch(config)#int f0/1  
 Switch(config-if)#switchport mode trunk 配置Trunk链路

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down  
 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up  
 Switch(config-if)#exit  
 Switch(config)#vlan 2 创建VLAN 2  
 Switch(config-vlan)#name gongchengbu vlan2为工程部  
 Switch(config-vlan)#exit  
 Switch(config)#vlan 3 创建VLAN 3  
 Switch(config-vlan)#name caiwubu VLAN3为财务部  
 Switch(config-vlan)#exit  
 Switch(config-vlan)#vlan 4 创建VLAN 4  
 Switch(config-vlan)#name jishubu VLAN4为技术部  
 Switch(config-vlan)#exit  
 Switch(config)#int f0/2  
 Switch(config-if)#switchport access vlan 2 给VLAN 2手工添加成员  
 Switch(config-if)#exit  
 Switch(config)#int f0/3  
 Switch(config-if)#switchport access vlan 2  
 Switch(config-if)#exit  
 Switch(config)#int f0/4  
 Switch(config-if)#switchport access vlan 3 给VLAN 3手工添加成员  
 Switch(config-if)#exit  
 Switch(config)#int f0/5  
 Switch(config-if)#switchport access vlan 3  
 Switch(config-if)#exit  
 Switch(config)#int f0/6  
 Switch(config-if)#switchport access vlan 4 给VLAN 3手工添加成员  
 Switch(config-if)#exit  
 Switch(config)#int f0/7  
 Switch(config-if)#switchport access vlan 4  
 Switch(config-if)#exit

定义访问控制列表  
 定义访问控制列表时要细心，要把最特殊的访问控制列表放在最上面[。](http://www.pcjx.com)（在此例中，允许一台特定主机而拒绝一个网段，所以要把拒绝主机放在上面）[。](http://www.pcjx.com)  
 注意：要想一个访问列表能够得到应用，必须在接口绑定[。](http://www.pcjx.com)

R1

r1(config)#access-list 10 permit 192.168.2.2 0.0.0.0  
 r1(config)#access-list 10 deny 192.168.2.0 0.0.0.255  
 r1(config)#access-list 10 permit 192.168.3.2 0.0.0.0  
 r1(config)#access-list 10 deny 192.168.3.0 0.0.0.255  
 r1(config)#access-list 10 permit any  
 r1(config)#int f0/0.1  
 r1(config-subif)#ip access-group 10 out  
 r1(config-subif)#exit  
 r1(config)#access-list 11 permit 192.168.1.2 0.0.0.0  
 r1(config)#access-list 11 deny 192.168.1.0 0.0.0.255  
 r1(config)#access-list 11 permit 192.168.3.2 0.0.0.0  
 r1(config)#access-list 11 deny 192.168.3.0 0.0.0.255  
 r1(config)#access-list 11 permit any  
 r1(config)#int f0/0.2  
 r1(config-subif)#ip access-group 11 out  
 r1(config-subif)#exit  
 r1(config)#access-list 12 permit 192.168.1.2 0.0.0.0  
 r1(config)#access-list 12 deny 192.168.1.0 0.0.0.255  
 r1(config)#access-list 12 permit 192.168.2.2 0.0.0.0  
 r1(config)#access-list 12 deny 192.168.2.0 0.0.0.255  
 r1(config)#access-list 12 permit any  
 r1(config)#int f0/0.3  
 r1(config-subif)#ip access-group 12 out  
 r1(config-subif)#exit

OK了，现在通过配置后所有的员工都能与互联网通讯[。](http://www.pcjx.com)（由于主机较多就不一一列述）

PC>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time=94ms TTL=254  
 Reply from 172.16.1.2: bytes=32 time=94ms TTL=254  
 Reply from 172.16.1.2: bytes=32 time=94ms TTL=254  
 Reply from 172.16.1.2: bytes=32 time=90ms TTL=254

Ping statistics for 172.16.1.2:  
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
 Approximate round trip times in milli-seconds:  
 Minimum = 90ms, Maximum = 94ms, Average = 93ms

配置完成后，PC 1 、PC 3 和 PC5之间，即每个部门的部门经理之间能相互通信[。](http://www.pcjx.com)

PC1 ping PC3

PC1>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=125ms TTL=127  
 Reply from 192.168.2.2: bytes=32 time=110ms TTL=127  
 Reply from 192.168.2.2: bytes=32 time=110ms TTL=127  
 Reply from 192.168.2.2: bytes=32 time=125ms TTL=127

Ping statistics for 192.168.2.2:  
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
 Approximate round trip times in milli-seconds:  
 Minimum = 110ms, Maximum = 125ms, Average = 117ms

PC1 PING PC5

PC1>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=111ms TTL=127  
 Reply from 192.168.3.2: bytes=32 time=120ms TTL=127  
 Reply from 192.168.3.2: bytes=32 time=111ms TTL=127  
 Reply from 192.168.3.2: bytes=32 time=105ms TTL=127

Ping statistics for 192.168.3.2:  
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
 Approximate round trip times in milli-seconds:  
 Minimum = 105ms, Maximum = 120ms, Average = 111ms

PC3 PING PC5

PC3>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=125ms TTL=127  
 Reply from 192.168.3.2: bytes=32 time=125ms TTL=127  
 Reply from 192.168.3.2: bytes=32 time=109ms TTL=127  
 Reply from 192.168.3.2: bytes=32 time=94ms TTL=127

Ping statistics for 192.168.3.2:  
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
 Approximate round trip times in milli-seconds:  
 Minimum = 94ms, Maximum = 125ms, Average = 113ms

PC2 PC4和 PC6之间，即普通员工之间是不能相互通信的[。](http://www.pcjx.com)

PC 2 PING PC4

PC2>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.  
 Request timed out.  
 Request timed out.  
 Request timed out.

Ping statistics for 192.168.2.3:  
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC2 PING PC6

PC2>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.  
 Request timed out.  
 Request timed out.  
 Request timed out.

Ping statistics for 192.168.3.3:  
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC 4 PING PC 6

PC4>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.  
 Request timed out.  
 Request timed out.  
 Request timed out.

Ping statistics for 192.168.3.3:  
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

通过以上所有的配置，我们达到了目的：所有的员工通过一个公网地址与互联网通讯;使各部门经理之间能相互通信，普通员工之间不能相互通信[。](http://www.pcjx.com)