AR2220 加 S5700 联通外网的例子,在 S5700 下划分了三个 vlan,vlan100 连接路由器,别的两个 vlan 都可以访问外网,vlan 之间默认是互通的，就是把 VLAN、静态路由、默认路由、NAT、ACL 综合了一下，适合初学者，也适合小型网络的搭建，遇到类似的朋友可以进行参考。

掌握目标

一、交换机配置

（1）VLAN 划分与接口加入

（2）VLAN 接口定义

（3）默认路由

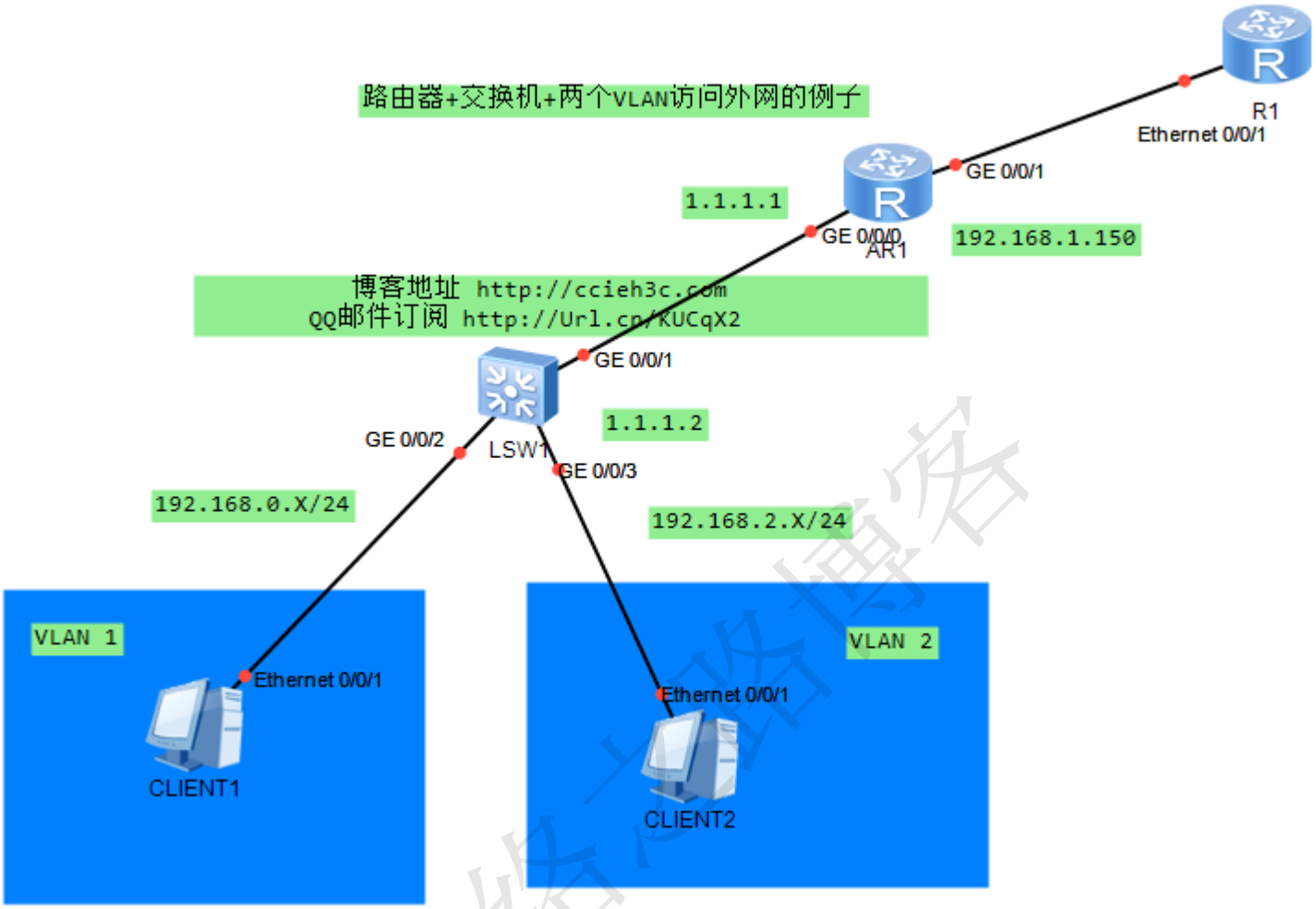
（4）DHCP 配置

二、路由器配置

（1）静态/默认路由配置

（2）NAT 配置

拓扑



1、三层交换机配置

【创建 VLAN 需要】

[HW-SW]vlan batch 2 100

【把接口加入到对应的 VLAN】

[HW-SW]int g0/0/3

[HW-SW-GigabitEthernet0/0/3]port link-type access

[HW-SW-GigabitEthernet0/0/3]port default vlan 2

[HW-SW]int g0/0/1

[HW-SW-GigabitEthernet0/0/1]port link-type access

[HW-SW-GigabitEthernet0/0/1]port default vlan 100

说明 :默认的情况下 ,G0/0/1 输入 VLAN 1 ,所以不需要修改 ,而 G0/0/3 则连接出口路由器的接口 ,划入到对应的 VLAN 100。

【创建 VLANIF 接口，作为对应 VLAN 的网关】

[HW-SW]int Vlanif 1

[HW-SW-Vlanif1]ip address 192.168.0.254 24

[HW-SW]int Vlanif 2

[HW-SW-Vlanif2]ip address 192.168.2.254 24

[HW-SW]int vlan 100

[HW-SW-Vlanif100]ip address 1.1.1.2 24

【DHCP 配置，让客户获取到地址】

[HW-SW]dhcp enable

[HW-SW]int vlan 1

[HW-SW-Vlanif1]dhcp select interface

[HW-SW-Vlanif1]

[HW-SW-Vlanif1]dhcp server dns-list 114.114.114.114

[HW-SW-Vlanif1]dhcp server domain-name ccieh3c.taobao.com

[HW-SW]int vlan 2

[HW-SW-Vlanif2]dhcp select interface

[HW-SW-Vlanif2]dhcp server dns-list 114.114.114.114

[HW-SW-Vlanif2]dhcp server domain-name ccieh3c.taobao.com

【默认路由配置】

[HW-SW]ip route-static 0.0.0.0 0 1.1.1.1

说明：接入客户的交换机配置内容其实很简单（1）配置 VLAN，并且让接口输入该 VLAN，这样 PC 发送的流量就只发送到该 VLAN 内处理。（2）每个 VLAN 的 VLANIF 接口配置，它们主要作为三层网关的通信，每个 VLAN 一个子网，每个子网有一个网关，PC 上面定义的网关就是为 VLANIF 接口 （3）DHCP 服务，如果客户端比较多，手动配置地址很麻烦，所以这里采用 DHCP 动态分配地址，DNS、域名等参数 （4）默认路由，由于 PC 最终需要访问其他网络或者外网，它们会把数据包发给三层交换机处理，交换机必须把数据包交给网关，而且出口只有一个，所以用默认路由来匹配是最合适的。

想系统的学习 DHCP，可以看 **DHCP 原理及在企业中的应用**

2、出口路由器配置

【配置接口地址】

[HW-GW]int g0/0/0

[HW-GW-GigabitEthernet0/0/0]ip address 1.1.1.1 24

[HW-GW]int g0/0/1

[HW-GW-GigabitEthernet0/0/1]ip address 192.168.1.150 24

【路由配置】

[HW-GW]ip route-static 192.168.0.0 24 1.1.1.2

[HW-GW]ip route-static 192.168.2.0 24 1.1.1.2

[HW-GW]ip route-static 0.0.0.0 0 192.168.1.254

说明：前面 2 条是做回程路由，当数据包从网关返回的时候，知道发给哪个设备。第三条路由则是访问外网的时候全部发往外网设备。

【NAT 配置】

.定义 ACL，匹配内网网段，做 NAT 转换

[HW-GW]acl number 3000

[HW-GW-acl-adv-3000]rule permit ip source 192.168.0.0 0.0.0.255

[HW-GW-acl-adv-3000]rule permit ip source 192.168.2.0 0.0.0.255

.外网口配置 easy-ip，关联 ACL 3000

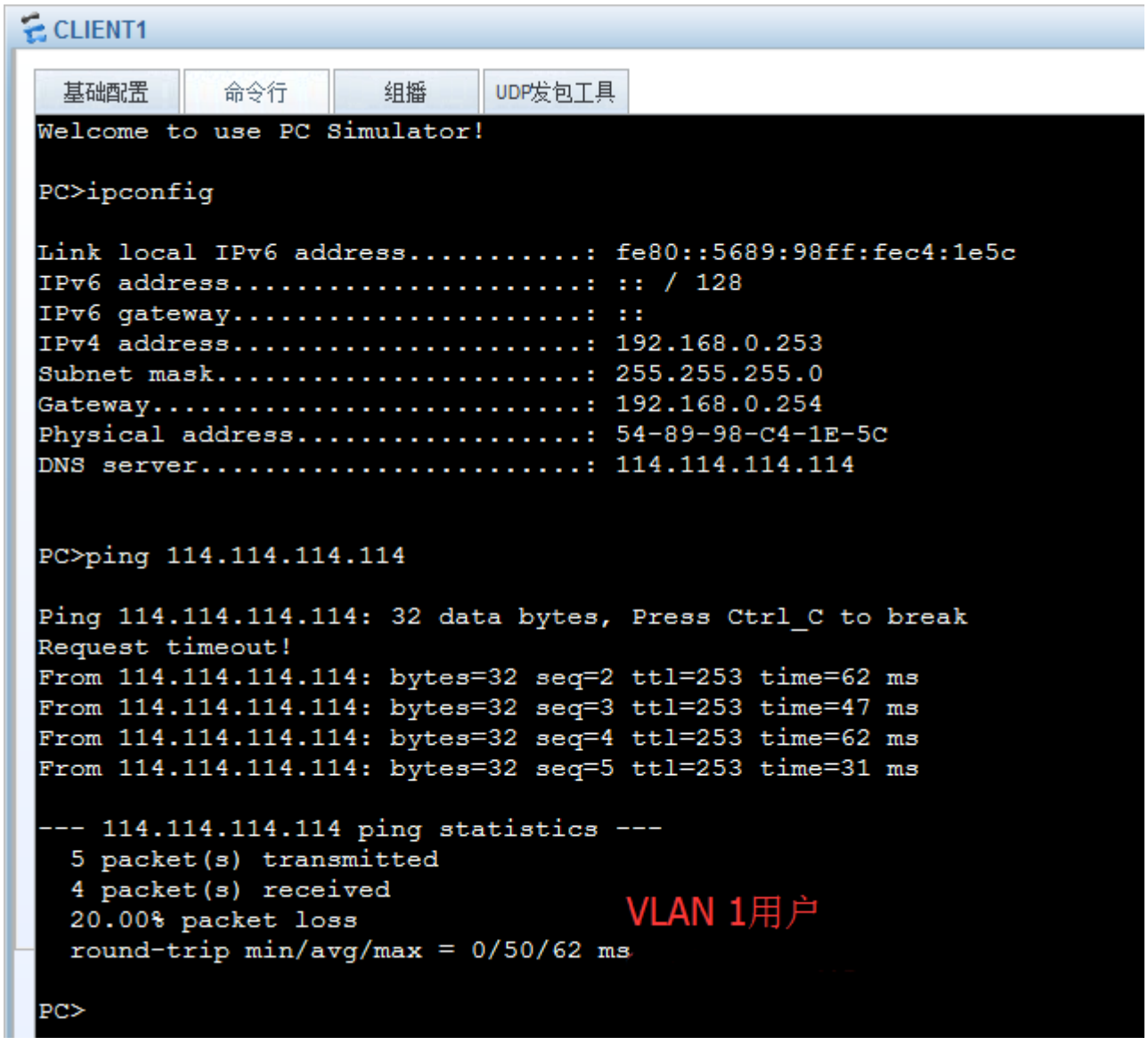
[HW-GW]int g0/0/1

[HW-GW-GigabitEthernet0/0/1]nat outbound 3000

说明：作用就是当匹配了 ACL 3000 里面的 rule 的时候，可以把源地址转换成出接口地址访问 internet。

三、验证

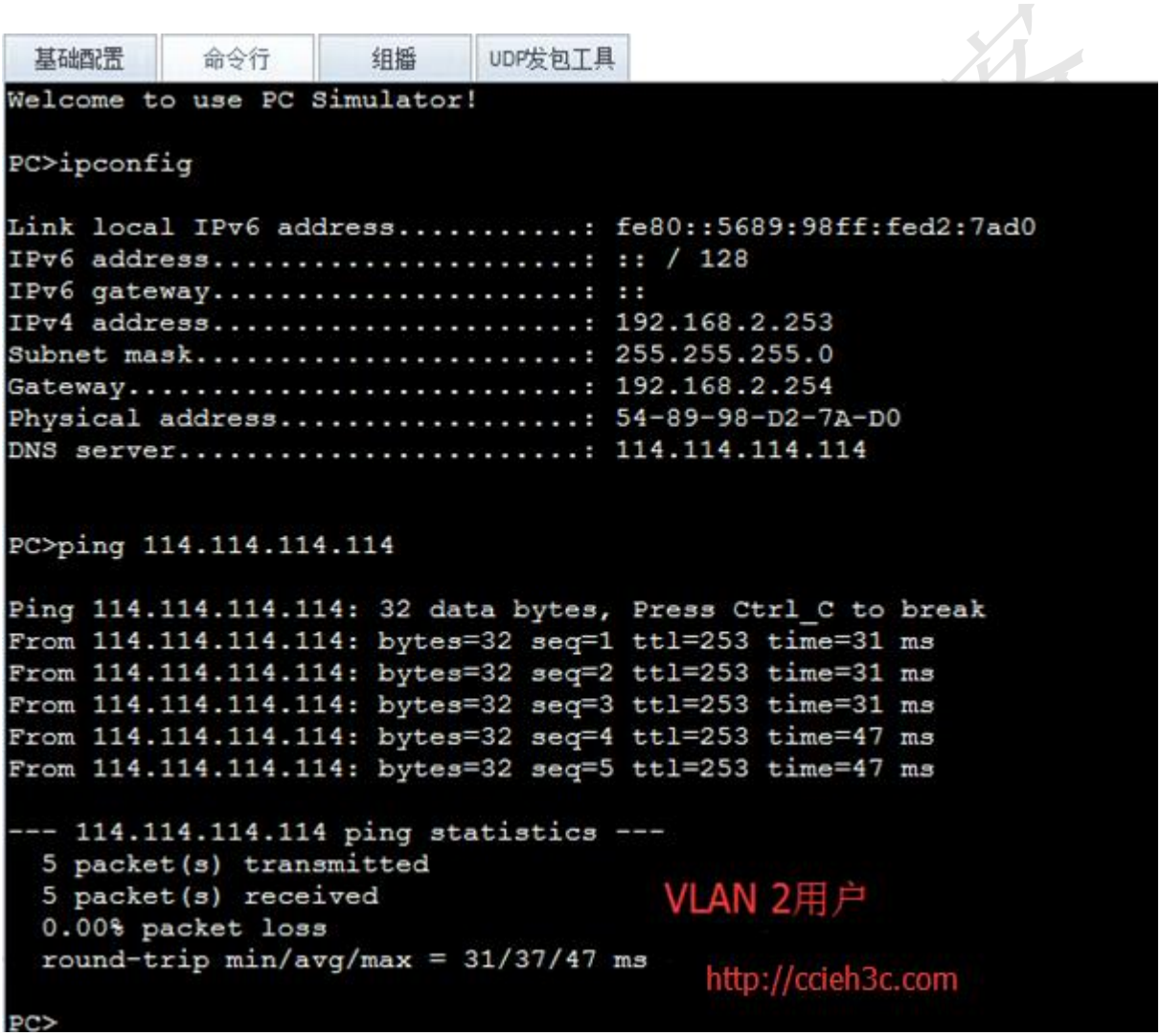
（1）VLAN 1 的用户测试



```
  Total : 0
<ccieh3c.qzone.qq.com-GW>display nat session all
  NAT Session Table Information:

     Protocol           : ICMP(1)
     SrcAddr    Vpn     : 192.168.0.253
     DestAddr   Vpn     : 114.114.114.114
     Type Code IcmpId   : 0    8    45292
     NAT-Info
       New SrcAddr      : 192.168.1.150
       New DestAddr     : ----
       New IcmpId       : 10240
```

可以看到 VLAN 1 的 PC 已经获取到了 IP，并且网关跟 DNS 都有，访问 114.114.114.114 也访问了，而且 NAT 有转换项。

（2）VLAN 2 的用户测试



```
Total : 0
<ccieh3c.qzone.qq.com-GW>display nat session all
 NAT Session Table Information:

     Protocol           : ICMP(1)
     SrcAddr    Vpn     : 192.168.2.253
     DestAddr   Vpn     : 114.114.114.114
     Type Code IcmpId   : 0    8    45582
     NAT-Info
       New SrcAddr      : 192.168.1.150
       New DestAddr     : ----
       New IcmpId       : 10250
```

同样访问木有问题。

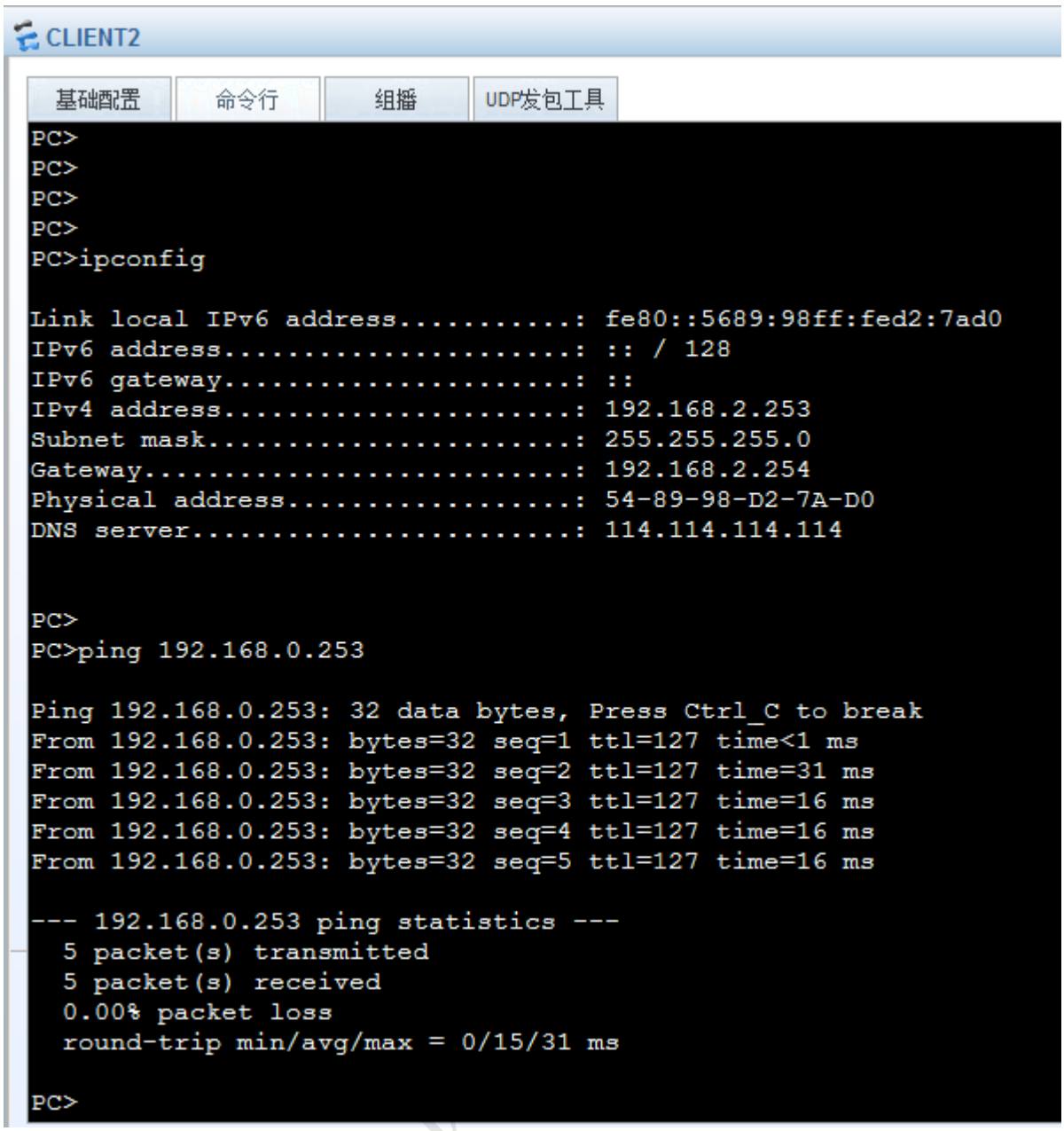
（3）VLAN 1 与 VLAN 2 之间的用户互访

CLIENT1

基础配置 | 命令行 | 组播 | UDP发包工具

```
  20.00% packet loss
  round-trip min/avg/max = 0/50/62 ms

PC>
PC>ipconfig

Link local IPv6 address.....: fe80::5689:98ff:fec4:1e5c
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.0.253
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.0.254
Physical address.....: 54-89-98-C4-1E-5C
DNS server.....: 114.114.114.114


PC>
PC>ping 192.168.2.253

Ping 192.168.2.253: 32 data bytes, Press Ctrl_C to break
From 192.168.2.253: bytes=32 seq=1 ttl=127 time=16 ms
From 192.168.2.253: bytes=32 seq=2 ttl=127 time=16 ms
From 192.168.2.253: bytes=32 seq=3 ttl=127 time=16 ms
From 192.168.2.253: bytes=32 seq=4 ttl=127 time=31 ms
From 192.168.2.253: bytes=32 seq=5 ttl=127 time=15 ms

--- 192.168.2.253 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/18/31 ms

PC>
```


VLAN 1访问VLNA 2



策略限制

如果要限制 VLAN 1 VLAN 2 的用户 可以通过端口隔离技术实现，是限制 VLAN 1 VLAN2 的部分用户之间不能互访，则必须通过 ACL。这两个可以具体参考下面的汇总系列，有端口隔离以及 ACL 的详细讲解。

博主也只是业余时间写写技术文档，请大家见谅，大家觉得不错的话，可以推荐给朋友哦，博主会努力推出更好的系列文档的。

如果大家有任何疑问或者文中有错误跟疏忽的地方，欢迎大家留言指出，博主看到后会第一时间修改，谢谢大家的支持，更多