

大多数人学习内网的过程其实并不系统，我也是这么过来的，这和日站的流程有关。往往搞安全的都是先从外网打点进去，然后再打内网。然后内网大多数时候就是 fscan 一把梭，然后找双网卡机器，找邮服等等。这些方法有用，但是较为片面，遇到限制强的网络环境就会有问题，例如网闸隔断，例如 acl 强限制，例如出口限制等。这些问题，很多时候也没解决，就放着。这就导致，打内网的经验累积，仅仅局限于打设备，打域上，实际上整个内网运行和隔断的机制，很多人并不了解。然后周而复始，内网技术一直得不到很大提升。

其实还是方法问题，要搞安全，首先得懂他是怎么开发出来的，这一点和代码审计类似。外界有时候戏称，进内网像回家一样。一个地方之所以能被称为家，那么家里的每个东西是不是都非常熟悉，基本都是自己搞回来的，自己也知道是干啥的。因此要搞内网安全，首先要懂内网是怎么搭建起来的，也就是得学习组网技术。基本的组网看完之后，懂的七七八八了，然后再根据实战填充知识就行。这里我自己复习一遍，记录下全流程。这里预计是花两天的时间

---20220529 3:33---

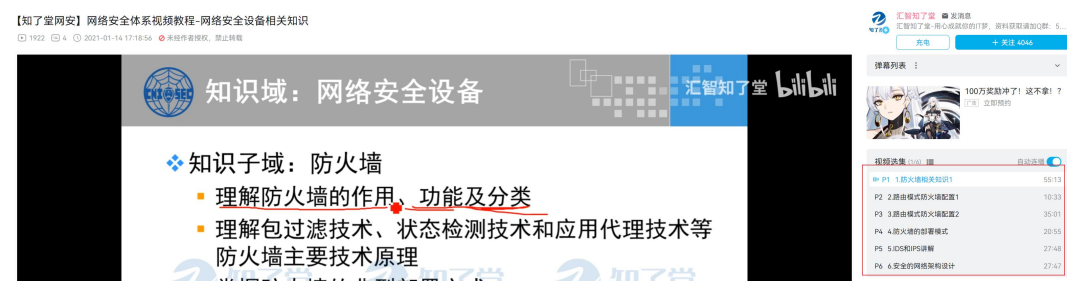
我的计划是  
先轮一遍基础

<https://www.bilibili.com/video/BV11r4y1J7wH?p=6>



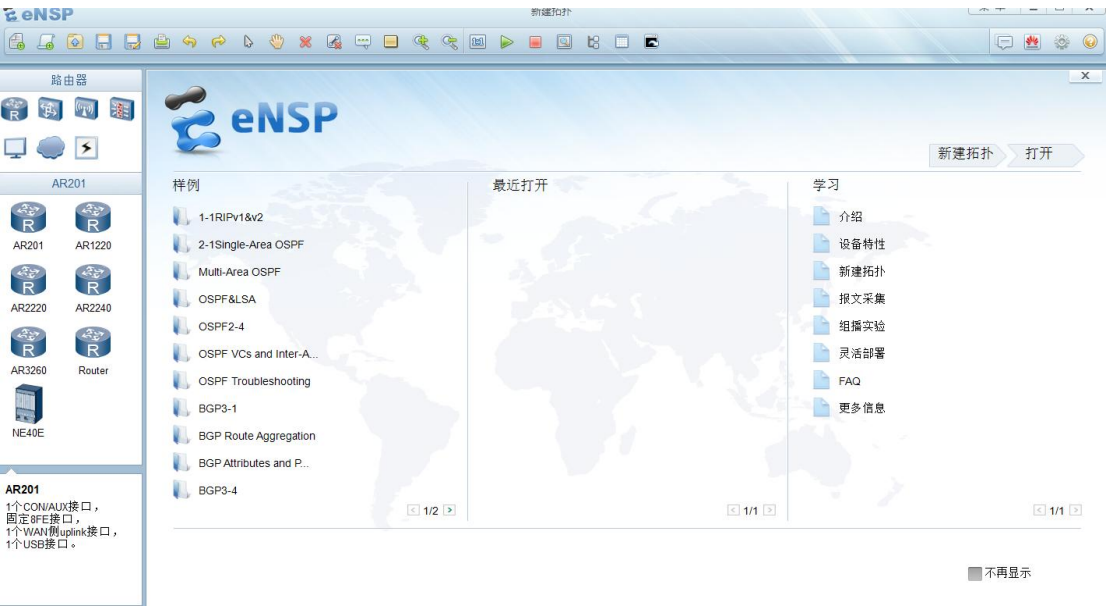
然后再单独看一篇安全设备篇

[bilibili.com/video/BV1Lp4y1x7Dj?spm\\_id\\_from=333.337.search-card.all.click](https://www.bilibili.com/video/BV1Lp4y1x7Dj?spm_id_from=333.337.search-card.all.click)

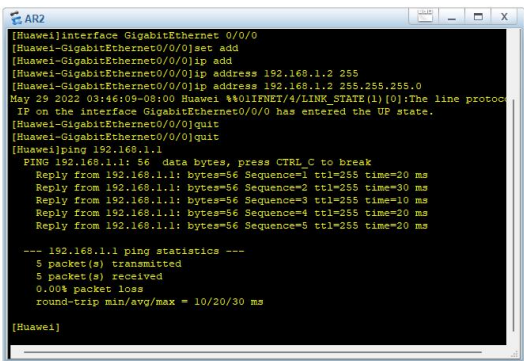
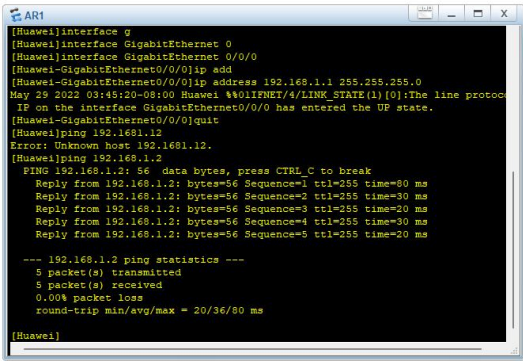
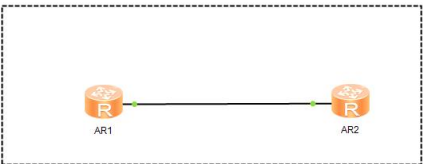


然后再来一篇关于域的 这里选的是 2008 的 域的不打算一次全部看完 用一点看一点 [https://www.bilibili.com/video/BV1pf4y197kj?spm\\_id\\_from=333.337.search-card.all.click](https://www.bilibili.com/video/BV1pf4y197kj?spm_id_from=333.337.search-card.all.click) 感觉基础基本够用了，实在不行，再到实战中补充。

这里提供了一个很好的工具



这个 ens 相当于一个组网的模拟器，然后可以模拟内网中各种设备。

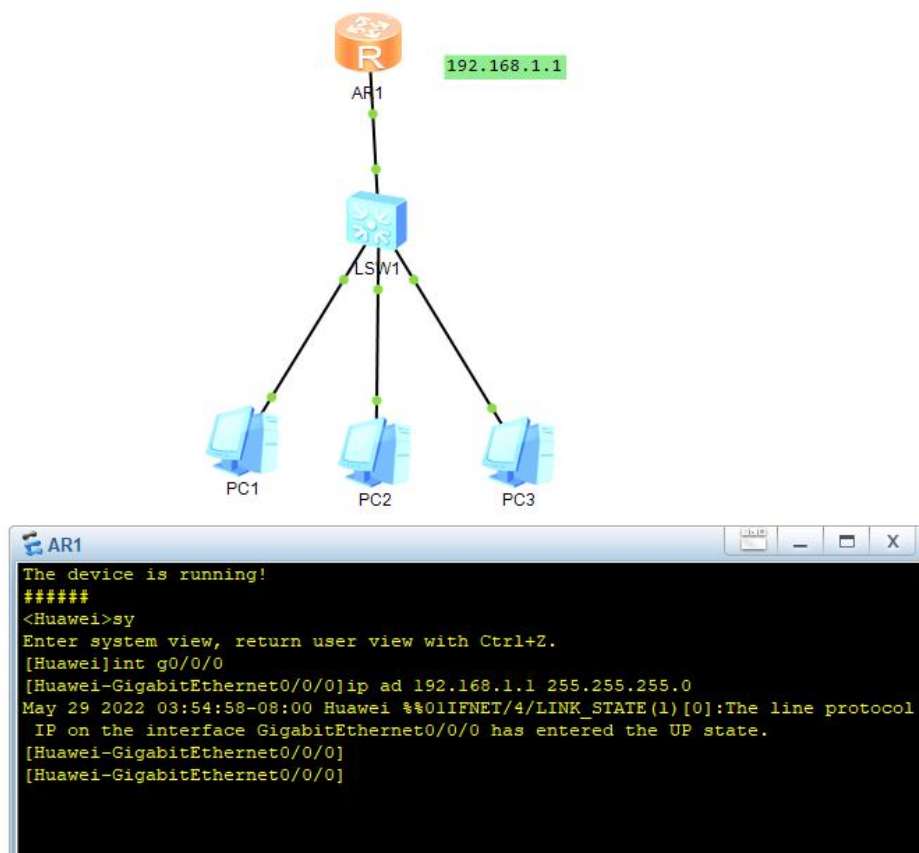


按照步骤配置两个路由器，然后进行 ping 检查

---2022-05-29 03:49:59.356326---

Dhcp

关注公众号：hack之道，回复关键词：2022，获取渗透工具、教程



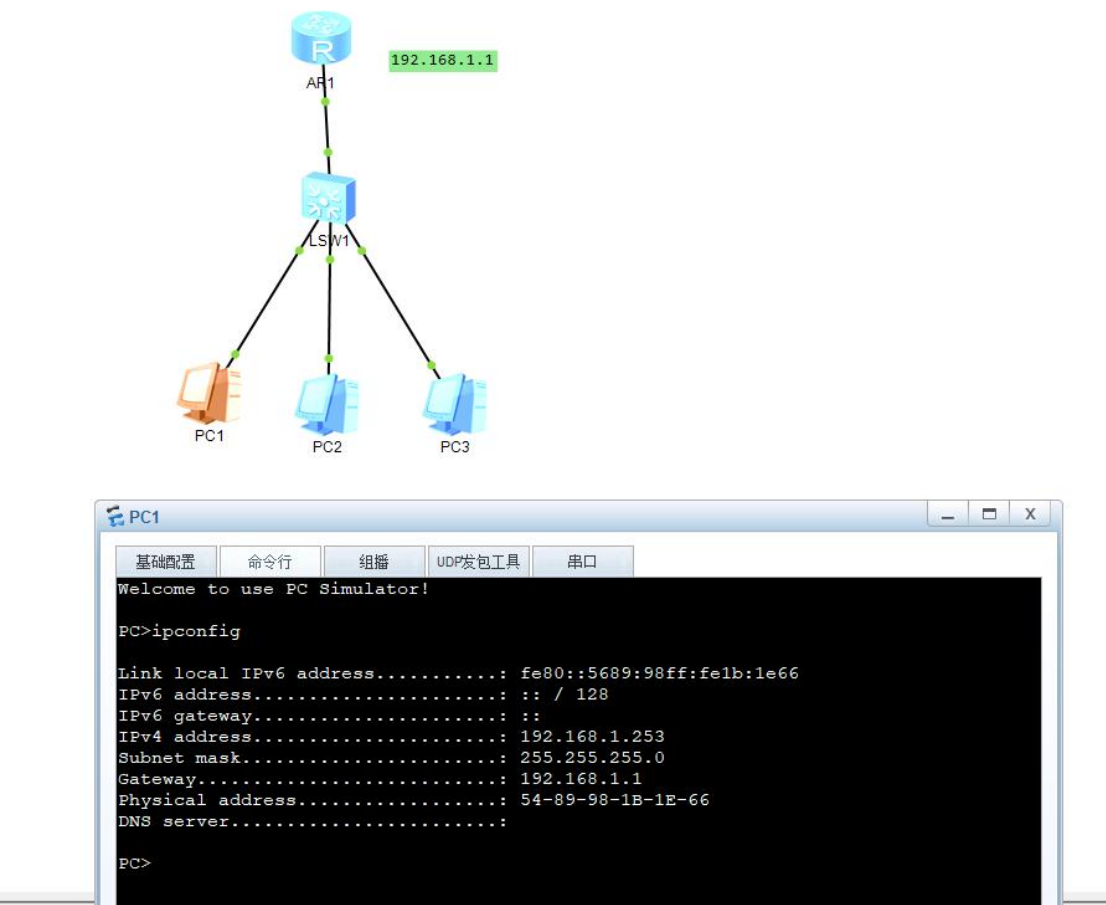
配置路由器地址

然后配一个 dhcp 服务器

```
[Huawei-GigabitEthernet0/0/0]ip ad 192.168.1.1 255.255.255.0
May 29 2022 03:54:58-08:00 Huawei %%01IFNET/4/LINK_STATE(1)[0]:The line protocol
IP on the interface GigabitEthernet0/0/0 has entered the UP state.
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]
[Huawei-GigabitEthernet0/0/0]q
[Huawei]dhcp ena
[Huawei]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[Huawei]int
[Huawei]interface g0/0/0/0
^
Error: Wrong parameter found at '^' position.
[Huawei]dhcp sele
[Huawei]interface g0/0/0
[Huawei-GigabitEthernet0/0/0]dhcp
[Huawei-GigabitEthernet0/0/0]dhcp se
[Huawei-GigabitEthernet0/0/0]dhcp select inte
[Huawei-GigabitEthernet0/0/0]dhcp select interface
[Huawei-GigabitEthernet0/0/0]
```

加我微信好友（stonefor345），拉你进2022护网微信交流群

然后打开 pc 机器测试，成功



贼简单

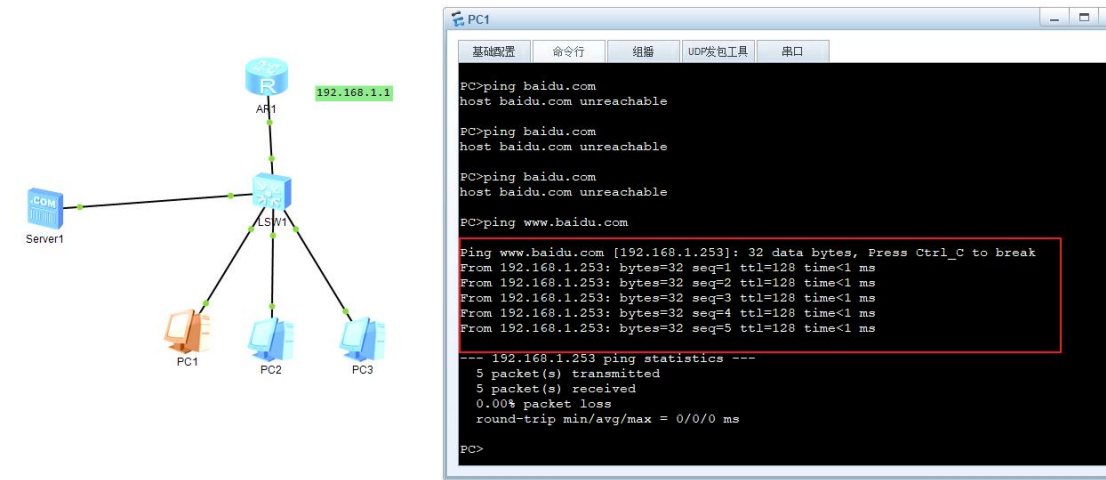
---2022-05-29 04:04:20.873530---

Dns 域名系统



先配置一个 baidu 的 dns 服务器

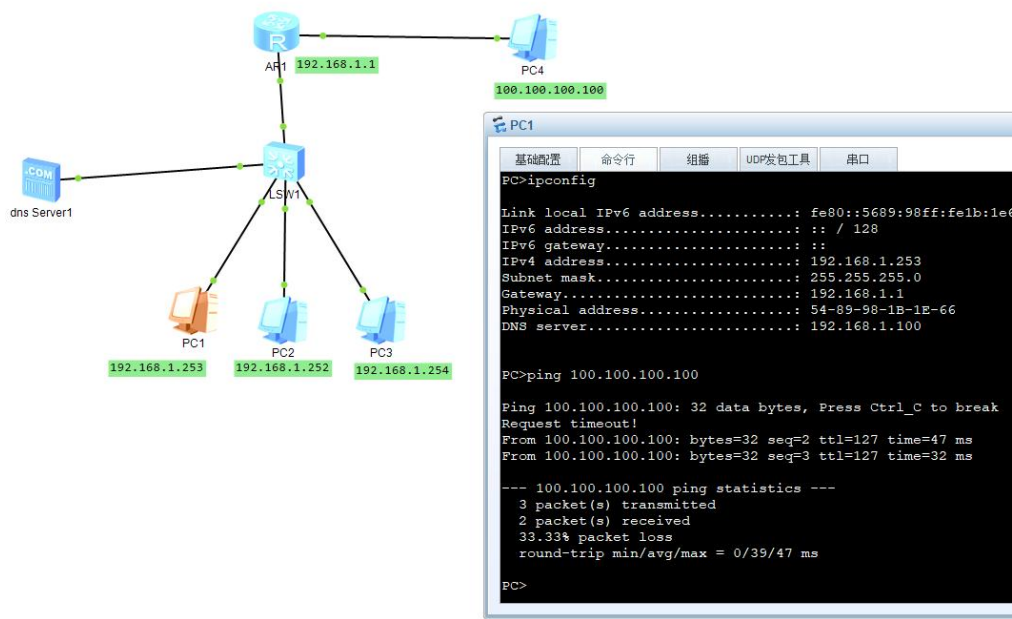
然后再到 dhcp 的那台机器上配置 dns 服务器所在地址，让 pc 机器可以去找最后达到的效果



---2022-05-29 04:16:20.759630---

路由技术基础

网关作用：用来连接不同的网段



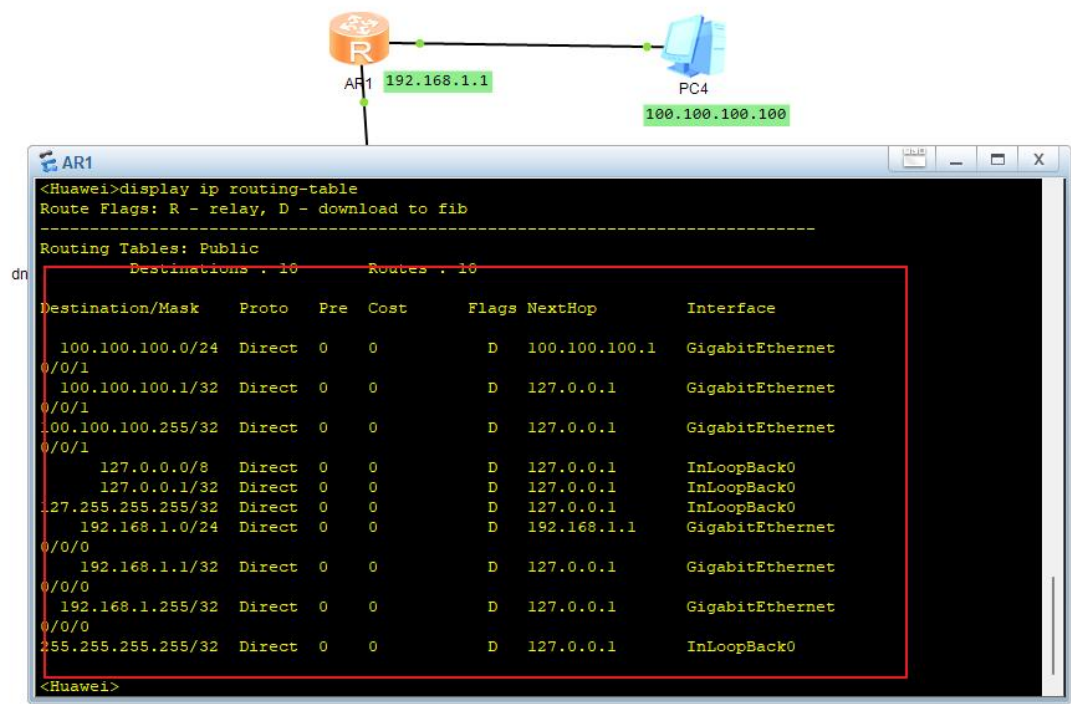
这里成功的用 192.168.1 段的机器 ping 通了 100.100.100.100 这台机器

就是因为在路由器中配置了 100.100.100.1 的网关，而路由起到了中间人的作用。

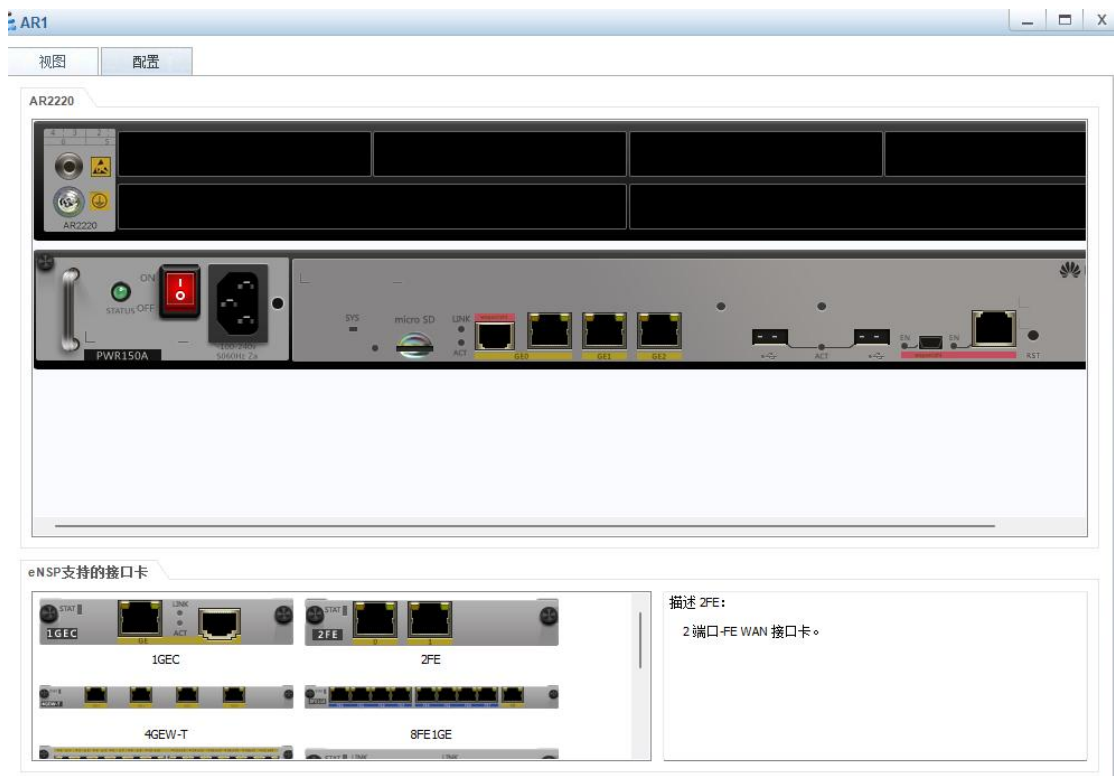
至于怎么找到了

查看路由器的路由表





路由器有很多不同的接口



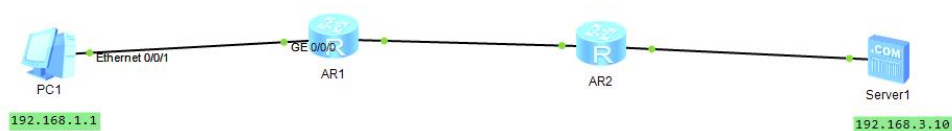
一个接口代表一条路

接口和网关对应，即可找到正确的路

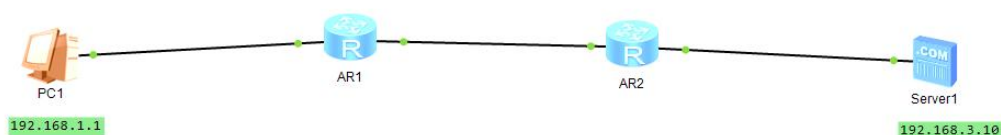
渗透的时候，也可以通过这个路由表找内网的网段。

---2022-05-29 04:32:18.503754---

静态路由



如上图所示，一个 ip 为 192.168.1.1 的机器  
需要通往一个 ip 为 192.168.3.10 的服务器  
这里需要通过两段路由进行转发  
一条是过去的路由  
一条是回来的路由  
两条都添加好了之后  
就可以 ping 通了



```
PC1
基础配置 命令行 组播 UDP发包工具 串口
From 192.168.3.1: bytes=32 seq=1 ttl=254 time=47 ms
From 192.168.3.1: bytes=32 seq=2 ttl=254 time=16 ms
From 192.168.3.1: bytes=32 seq=3 ttl=254 time=31 ms

--- 192.168.3.1 ping statistics ---
 3 packet(s) transmitted
 3 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 16/31/47 ms

PC>ping 192.168.3.10

Ping 192.168.3.10: 32 data bytes, Press Ctrl_C to break
From 192.168.3.10: bytes=32 seq=1 ttl=253 time=16 ms
From 192.168.3.10: bytes=32 seq=2 ttl=253 time=15 ms
From 192.168.3.10: bytes=32 seq=3 ttl=253 time=16 ms
From 192.168.3.10: bytes=32 seq=4 ttl=253 time=31 ms
From 192.168.3.10: bytes=32 seq=5 ttl=253 time=16 ms

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

PC>
```

成功 ping 通

---2022-05-29 07:10:21.313926---

Tcp&udp

基本原理直接过

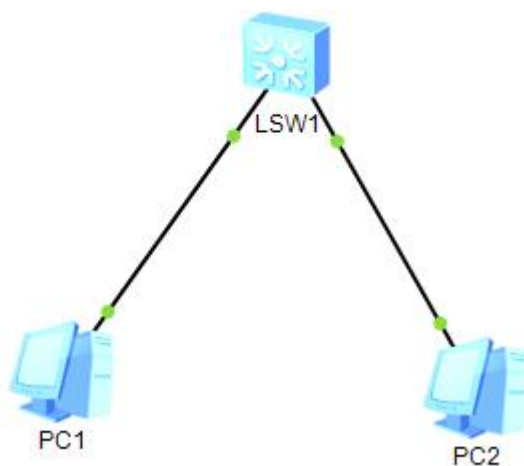
Tcp 可信

Udp 快

---2022-05-29 07:13:09.944764---

Vlan&acl

Vlan：虚拟隔离



基本模型

一开始能 ping 通

```
PC1
基础配置 命令行 组播 UDP发包工具 串口
PC>ping 1.1.1.2
Ping 1.1.1.2: 32 data bytes, Press Ctrl_C to break
From 1.1.1.2: bytes=32 seq=1 ttl=128 time=31 ms
From 1.1.1.2: bytes=32 seq=2 ttl=128 time=32 ms

--- 1.1.1.2 ping statistics ---
 2 packet(s) transmitted
 2 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/31/32 ms

PC>ping 1.1.1.2
Ping 1.1.1.2: 32 data bytes, Press Ctrl_C to break
From 1.1.1.1: Destination host unreachable
From 1.1.1.1: Destination host unreachable
From 1.1.1.1: Destination host unreachable

--- 1.1.1.2 ping statistics ---
 3 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>
```

The screenshot shows a terminal window titled 'PC1' with tabs for '基础配置', '命令行', '组播', 'UDP发包工具', and '串口'. The '命令行' tab is active. It shows two ping commands. The first, 'ping 1.1.1.2', is successful, showing two received packets with 0.00% loss. The second, also 'ping 1.1.1.2', fails, showing three transmitted packets but zero received, resulting in 100.00% packet loss. The source IP in the second ping is '1.1.1.1'.

配置了 vlan 之后，就不行了，相当于隔离了



```
## VLAN mapping,
# : ProtocolTransparent-vlan;
* : Management-vlan;

-----
VID  Type  Ports
-----
1    common  UT:GE0/0/3 (D)    GE0/0/4 (D)    GE0/0/5 (D)    GE0/0/6 (D)
                        GE0/0/7 (D)    GE0/0/8 (D)    GE0/0/9 (D)    GE0/0/10 (D)
                        GE0/0/11 (D)   GE0/0/12 (D)   GE0/0/13 (D)   GE0/0/14 (D)
                        GE0/0/15 (D)   GE0/0/16 (D)   GE0/0/17 (D)   GE0/0/18 (D)
                        GE0/0/19 (D)   GE0/0/20 (D)   GE0/0/21 (D)   GE0/0/22 (D)
                        GE0/0/23 (D)   GE0/0/24 (D)

10   common  UT:GE0/0/1 (U)
20   common  UT:GE0/0/2 (U)

-----
VID  Status  Property  MAC-LRN  Statistics  Description
-----
1    enable  default  enable  disable  VLAN 0001
10   enable  default  enable  disable  VLAN 0010
20   enable  default  enable  disable  VLAN 0020
[Huawei]
```

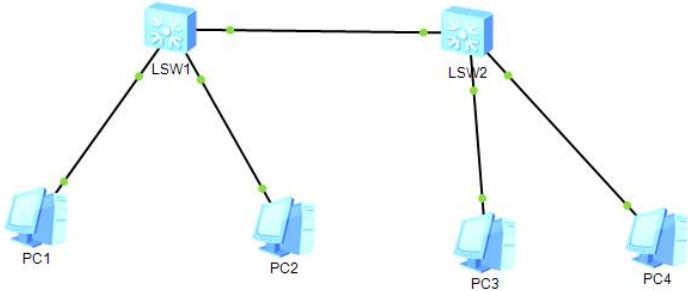
```
PC>ping 1.1.1.2

Ping 1.1.1.2: 32 data bytes, Press Ctrl_C to break
From 1.1.1.1: Destination host unreachable
From 1.1.1.1: Destination host unreachable
From 1.1.1.1: Destination host unreachable

--- 1.1.1.2 ping statistics ---
 3 packet(s) transmitted
 0 packet(s) received
100.00% packet loss
```

---2022-05-29 07:28:06.920973---

Trunk  
就是一个标签技术  
打上了标签，就能知道数据包来自于哪个 vlan



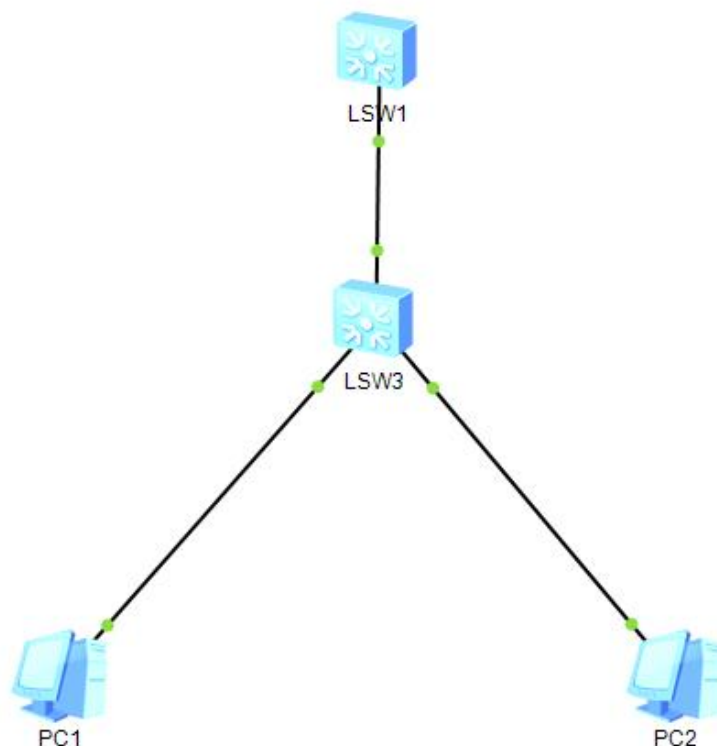
这里 pc1 可以通 pc3

---2022-05-29 07:39:38.609578---

三层交换技术

先用 vlan 把用户隔离开

然后再连接起来



一个三层的架构

能通信是因为最上面那台交换机

接口配置的网关互通

因此可以实现通信

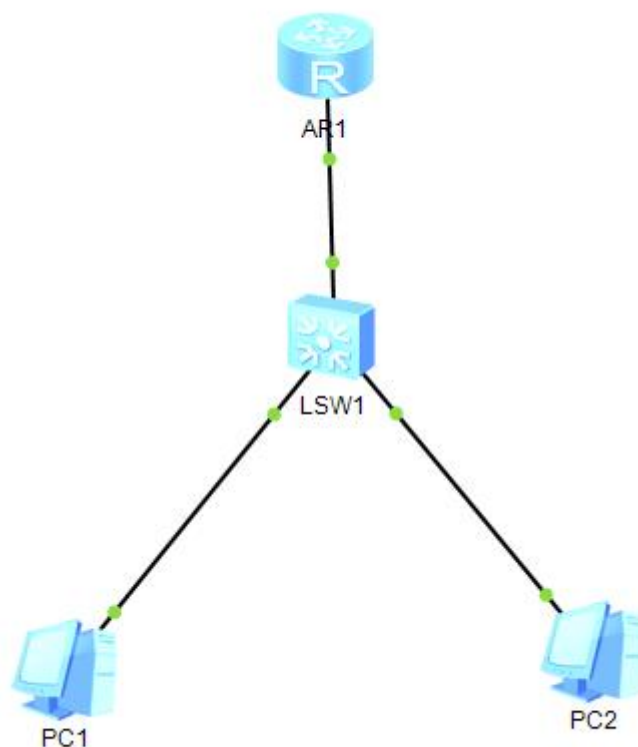
如果是单单用下面这台交换机

就是单纯的隔断

```
welcome to use PC Simulator!  
  
PC>ping 2.2.2.1  
  
Ping 2.2.2.1: 32 data bytes, Press Ctrl_C to break  
From 2.2.2.1: bytes=32 seq=1 ttl=127 time=172 ms  
From 2.2.2.1: bytes=32 seq=2 ttl=127 time=94 ms  
  
--- 2.2.2.1 ping statistics ---  
 2 packet(s) transmitted  
 2 packet(s) received  
 0.00% packet loss  
 round-trip min/avg/max = 94/133/172 ms  
  
PC>
```

---2022-05-29 08:13:34.127425---

单臂路由



和三层交换机大差不差，都是为了做 vlan 之间的通信。

---2022-05-29 11:03:33.362201---

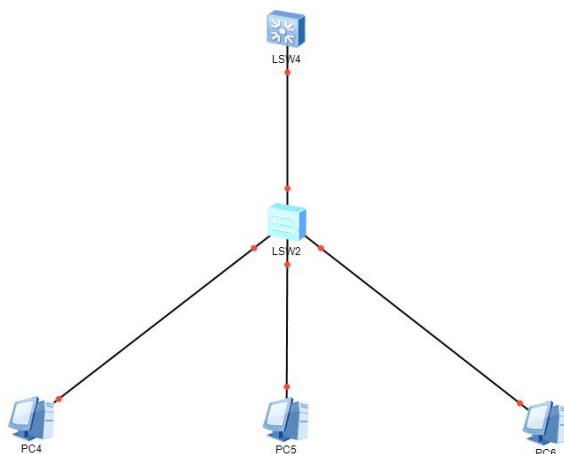
Acl 访问控制

使用方法

先建立一个规则

再调用这个规则

网络架构：



```
[Huawei-acl-adv-test]rule deny ip so  
[Huawei-acl-adv-test]rule deny ip source 192.168.10.0 0.0.0.255 I
```

关于 acl 的配置

这行就是拒绝对应 ip 的访问

写好规则之后

进行调用

```
lawei-GigabitEthernet0/0/1]traffic-filter inbound acl name test
```

这里就是在 0/0/1 节点调用这条规则

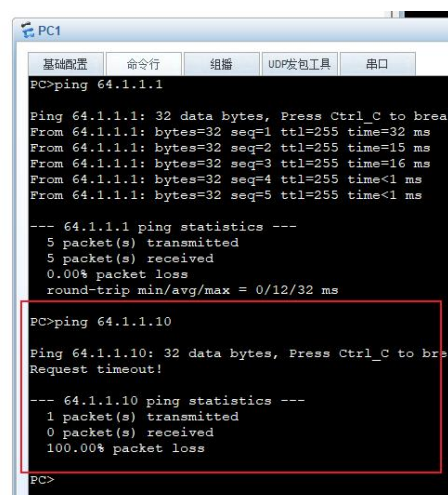
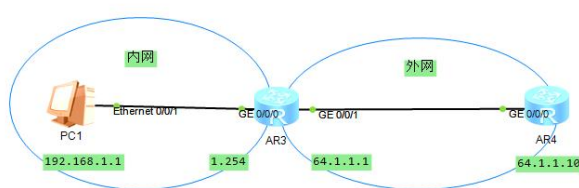
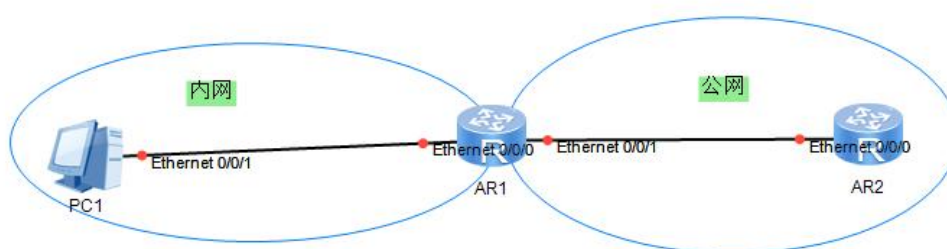
这里我太懒的，就不自己配置运行实验环境了，毕竟我也不是搞网络的。

这种原理了解即可，自己配置的情况应该很少。

---2022-05-29 11:25:54.438099---

NAT 网络地址转换

配置一个内网环境，一个公网环境



这里发现内网 ping 公网的 64.10 地址是不通的

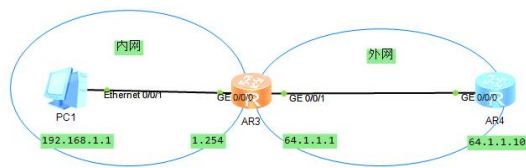
解决办法就是做 nat 网络地址转换

这里其实能出去

但是无法回包

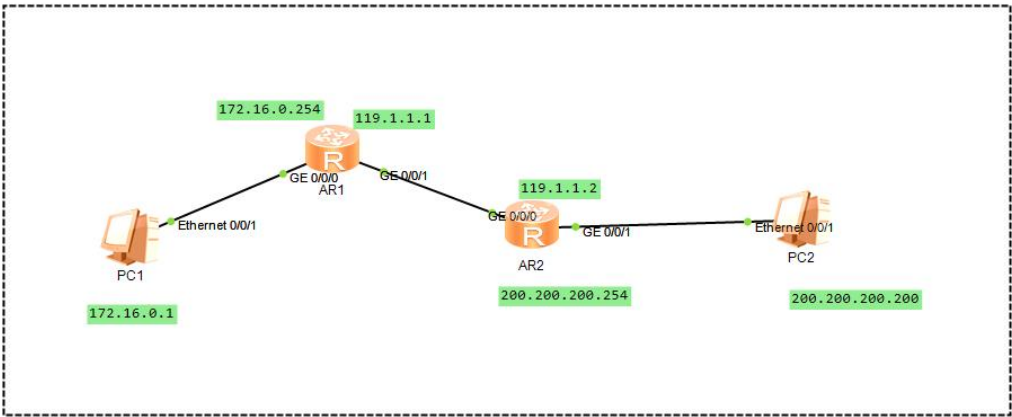
因此需要用 nat 来解决

配置完成后成功 ping 通



```
AR3
rule 5 permit source 192.168.0.0 0.0.255.255
Advanced ACL rule 5
ACL's step is 5
[Huawei-GigabitEthernet0/0/1]int g0/0/1
[Huawei-GigabitEthernet0/0/1]nat out
[Huawei-GigabitEthernet0/0/1]nat out
[Huawei-GigabitEthernet0/0/1]nat outbound 2000 address-group 1
[Huawei-GigabitEthernet0/0/1]ping 64.1.1.10
PING 64.1.1.10: 56 data bytes, press CTRL C to break
  Reply from 64.1.1.10: bytes=56 Sequence=1 ttl=255 time=60 ms
  Reply from 64.1.1.10: bytes=56 Sequence=2 ttl=255 time=20 ms
  Reply from 64.1.1.10: bytes=56 Sequence=3 ttl=255 time=20 ms
  Reply from 64.1.1.10: bytes=56 Sequence=4 ttl=255 time=30 ms
  Reply from 64.1.1.10: bytes=56 Sequence=5 ttl=255 time=20 ms
--- 64.1.1.10 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 20/30/60 ms
[Huawei-GigabitEthernet0/0/1]
```

---2022-05-29 14:23:54.187197---



这套架构是相当于内网有一台 server  
然后做一个 nat 映射到公网上给大家访问

---2022-05-29 14:38:13.123904---

远程管理网络设备



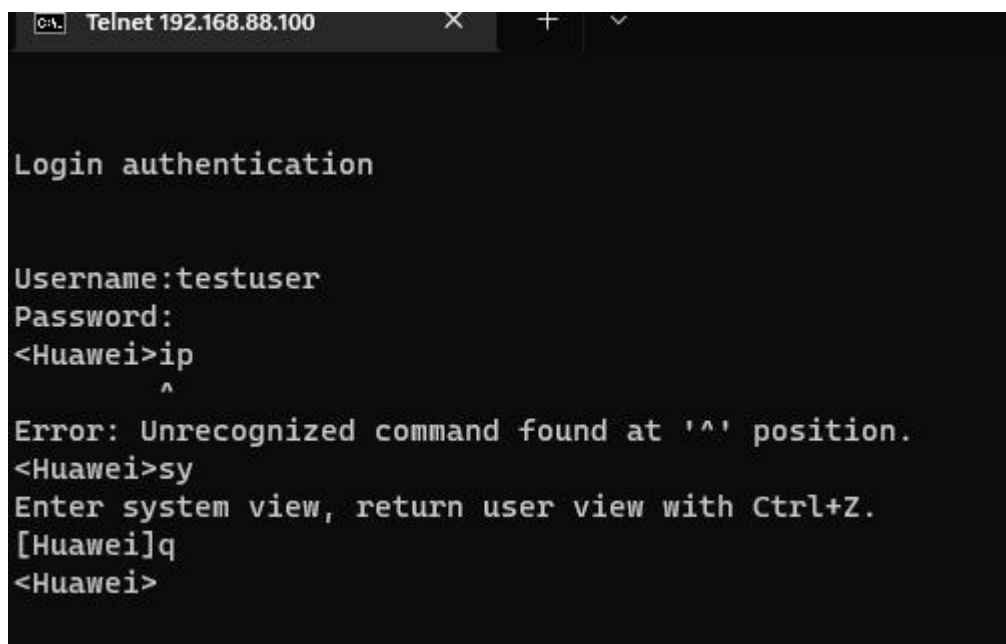
架构如上  
这里云相当于是本机  
这里用 telnet 连接  
先在路由器配置账号密码



关注公众号：hack之道，回复关键词：2022，获取渗透工具、教程

```
[Huawei-ui-vty0-4]au
[Huawei-ui-vty0-4]authentication-mode ^
Error:Incomplete command found at '^' position.
[Huawei-ui-vty0-4]au
[Huawei-ui-vty0-4]auth
[Huawei-ui-vty0-4]authentication-mode aaa
[Huawei-ui-vty0-4]aaa
[Huawei-aaa]lo
[Huawei-aaa]local-user testuser pa
[Huawei-aaa]local-user testuser password ci
[Huawei-aaa]local-user testuser password cipher 123456
Info: Add a new user.
[Huawei-aaa]loc
[Huawei-aaa]local-user te
[Huawei-aaa]local-user testuser pri
[Huawei-aaa]local-user testuser privilege lev
[Huawei-aaa]local-user testuser privilege level 15
[Huawei-aaa]lo
[Huawei-aaa]local-user test
[Huawei-aaa]local-user testuser ser
[Huawei-aaa]local-user testuser service-type tel
[Huawei-aaa]local-user testuser service-type telnet
[Huawei-aaa]q
[Huawei]tel
[Huawei]telnet ser
[Huawei]telnet server e
[Huawei]telnet server enable
Error: TELNET server has been enabled
[Huawei]
```

然后连接



```
C:\> Telnet 192.168.88.100

Login authentication

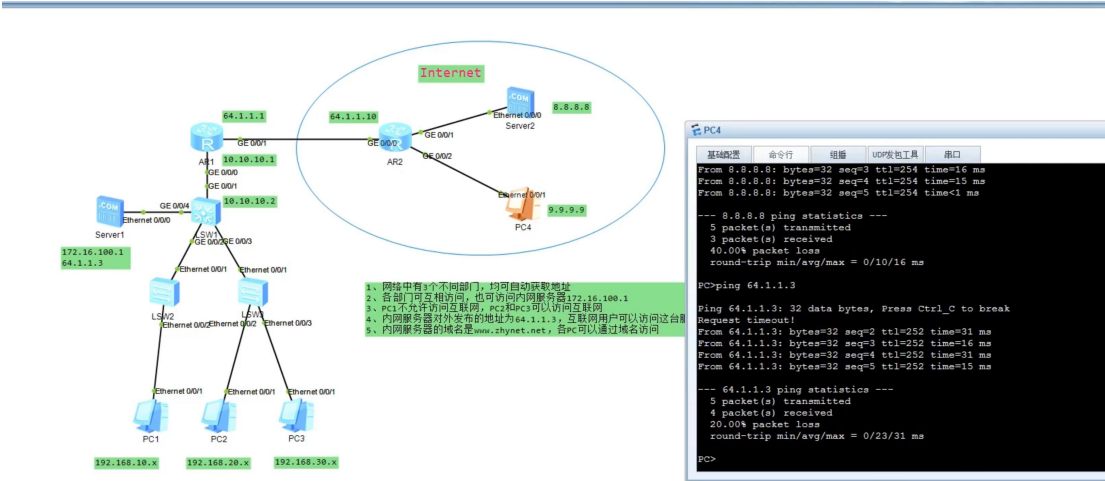
Username:testuser
Password:
<Huawei>ip
^
Error: Unrecognized command found at '^' position.
<Huawei>sy
Enter system view, return user view with Ctrl+Z.
[Huawei]q
<Huawei>
```

这里本机直接连接

---2022-05-29 14:54:40.688345---

综合项目

加我微信好友（stonefor345），拉你进2022护网微信交流群



这里直接搬运他的图 懒得配了 一堆重复的工作  
过程就是先划分 vlan 做隔离  
然后配置网关  
然后配置路由  
这里 pc1 不给出网  
于是路由上需要配置一个 acl 策略  
禁止源头出网

---2022-05-29 15:13:36.530577---

基础部分过完

下面开始看具体的设备篇

[bilibili.com/video/BV1Lp4y1x7Dj?spm\\_id\\_from=333.337.search-card.all.click](https://www.bilibili.com/video/BV1Lp4y1x7Dj?spm_id_from=333.337.search-card.all.click)

视频选集 (1/6) 自动连播

III P1

1.防火墙相关知识1

55:13

P2

2.路由模式防火墙配置1

10:33

P3

3.路由模式防火墙配置2

35:01

P4

4.防火墙的部署模式

20:55

P5

5.IDS和IPS讲解

27:48

P6

6.安全的网络架构设计

27:47

看了下他的配置  
主要涉及  
防火墙 ids ips 架构设计  
那还是按照他的顺序来看

关注公众号：hack之道，回复关键词：2022，获取渗透工具、教程

有点困了 不行 先去睡一会

加我微信好友（stonefor345），拉你进2022护网微信交流群