

B 级达标测试实验报告

计算机网络综合设计实验

2022 年 5 月 5 日

姓名	学号	学院	任务分工	贡献度	签名
王式政	19160100027	计算机科学与技术学院	方案设计， DHCP 配置，端口限流	40%	王式政
袁铮	19050400004	计算机科学与技术学院	ARP 泛洪和欺骗防护	30%	袁铮
李宇浩	19030100194	计算机科学与技术学院	拓扑建立和静态路由配置	30%	李宇浩

指导教师评语：

成 绩

测试教师：

____年____月____日

实验报告内容基本要求及参考格式

- 一、实验目的
- 二、实验所用仪器（或实验环境）
- 三、实验基本原理及步骤（或方案设计及理论计算）
- 四、实验数据记录（或仿真及软件设计）
- 五、实验结果分析及回答问题（或测试环境及测试结果）

一、测试内容

- 1、利用华为 eSNP 网络模拟器，搭建与图 1 相对应的网络拓扑。在实验拓扑中共有 3 个网段（网 1、网 2 和网 3），其网络参数参见表 1。每个网段使用 1 台交换机。
- 2、路由器 R1 连接网 1 与网 2，路由器 R2 连接网 2 与网 3。
- 3、按照要求对每台设备进行配置，最终保证所有设备的连通性。

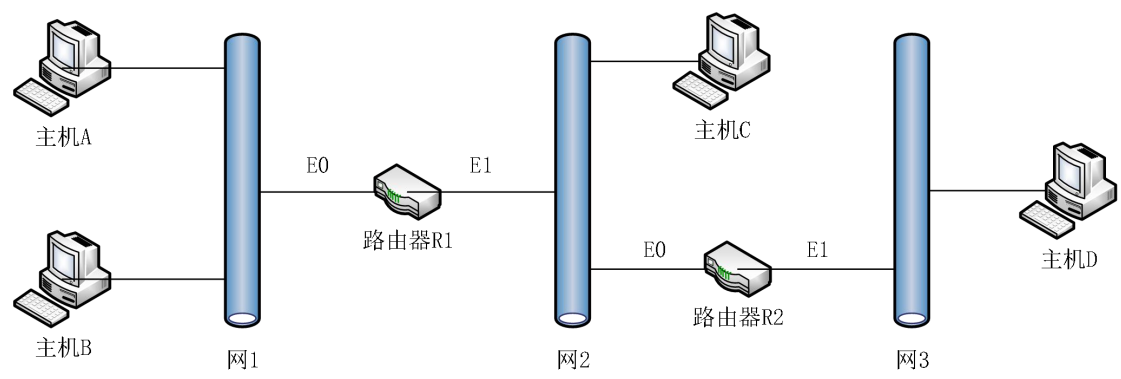


图 1实验拓扑

表 1网 1、网 2 与网 3 的网络参数

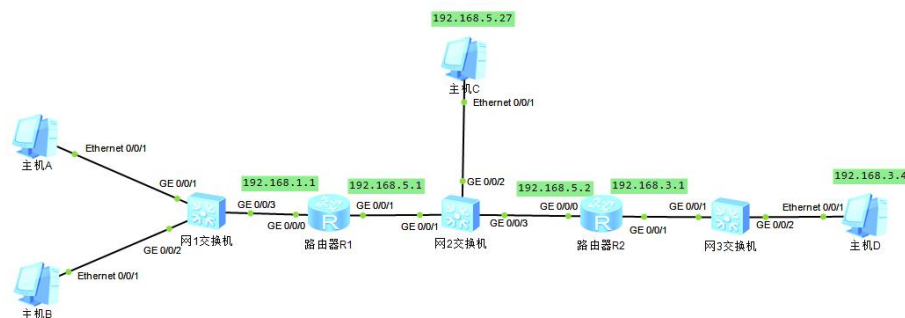
	子网掩码	网络号
网 1	255.255.255.0	192.168.1.0
网 2	255.255.255.0	192.168.5.0
网 3	255.255.255.0	192.168.3.0

二、测试要求

- 1、主机 A 与主机 B 的 IPv4 地址、子网掩码以及默认网关等参数由网络设备中的 DHCP 服务自动分配；
- 2、主机 C 和主机 D 的 IPv4 地址、子网掩码以及默认网关等参数由手动分配，且地址的最后一个字节必须设置为任一组员学号的后三位，否则测试不通过。
- 3、对主机 A 所连接的网络设备端口进行限速，其中入方向和出方向均限制为端口最大速率的 50%。
- 4、选择合适的网络设备，配置至少两种防 ARP 泛洪攻击功能以及至少两种防 ARP 欺骗攻击功能。

三、实验内容

实验拓扑图为：



静态路由的配置：

设置主机 C 和主机 D 的 IPv4 地址、子网掩码以及默认网关分别为 192.168.5.27 24 192.168.5.1 和 192.168.3.4 24 192.168.3.1

为路由器 R2 端口 GE0/0/0 和 GE0/0/1 配置 IP 地址：

```

路由器R2
路由器R1 路由器R2
The device is running!
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface gi 0/0/0
[R2-GigabitEthernet0/0/0]ip address 192.168.5.2 24
May  4 2022 17:41:13-08:00 R2 %01IFNET/4/LINK_STATE(1)[0]:The line protocol IP
on the interface GigabitEthernet0/0/0 has entered the UP state.
[R2-GigabitEthernet0/0/0]quit
[R2]interface gi 0/0/1
[R2-GigabitEthernet0/0/1]ip address 192.168.3.1 24
May  4 2022 17:41:48-08:00 R2 %01IFNET/4/LINK_STATE(1)[1]:The line protocol IP
on the interface GigabitEthernet0/0/1 has entered the UP state.

```

为路由器 R2 端口 GE0/0/0 和 GE0/0/1 配置 IP 地址：

```

interface GigabitEthernet0/0/0
ip address 192.168.1.1 255.255.255.0
dhcp select global
#
interface GigabitEthernet0/0/1
ip address 192.168.5.1 255.255.255.0
#

```

为路由器 R2 和路由器 R1 配置静态路由实现网段间的通信：

```

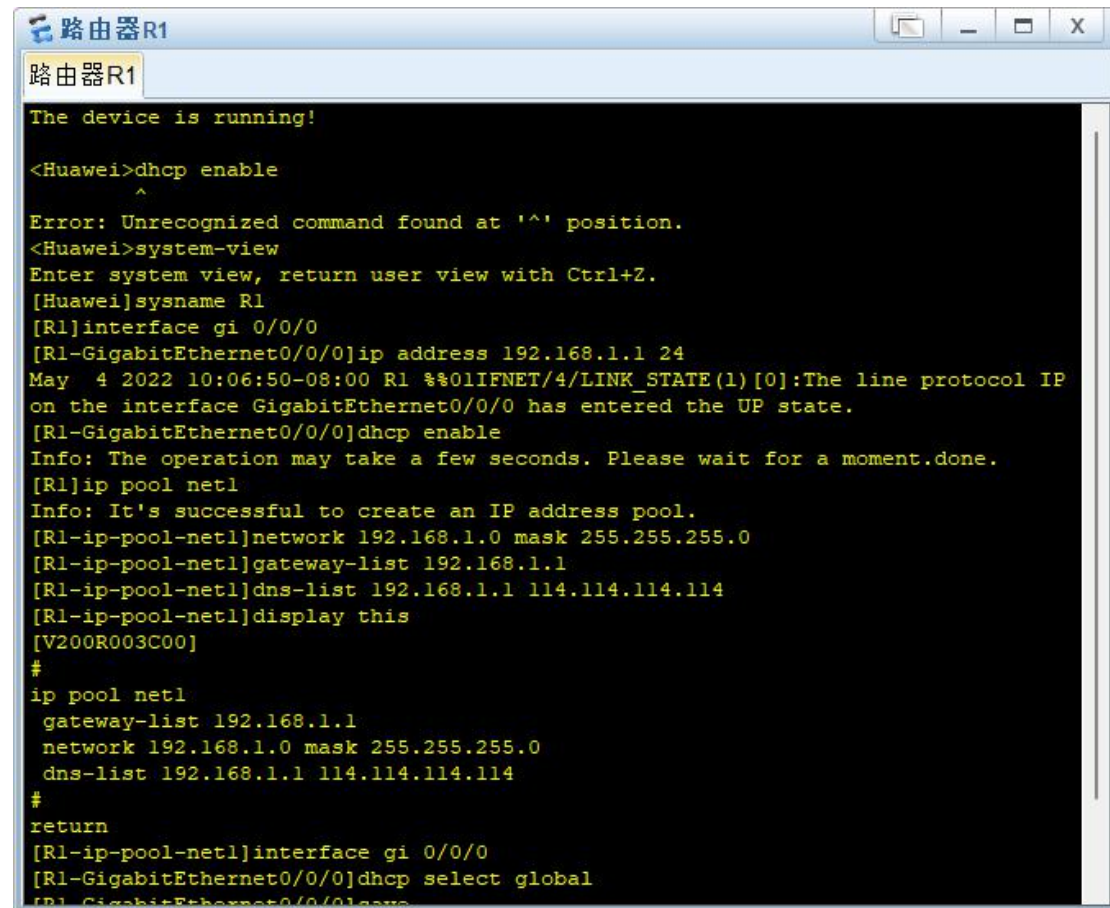
[R2-GigabitEthernet0/0/1]ip route-static 192.168.1.0 255.255.255.0 192.168.5.1
[R2]display current-configuration
[V200R003C00]

interface NULL0
#
ip route-static 192.168.3.0 255.255.255.0 192.168.5.2
#

```

接下来进行 DHCP 服务的配置：

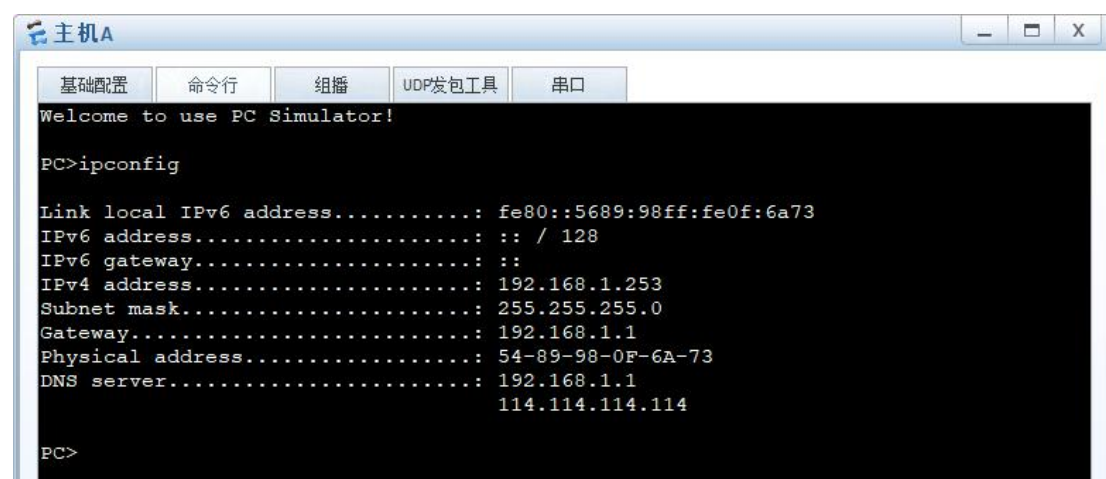
在路由器 R1 的系统配置模式下，先指定路由器 R1 GE0/0/0 接口的 ip 地址，启动 DHCP 服务，并设置基于全局模式的 DHCP 地址池。设定 DHCP 服务的对应网段、子网掩码和网关地址，并配置 DNS 服务器地址，设置 DHCP 基于全局配置。



```
路由器R1
The device is running!

<Huawei>dhcp enable
^
Error: Unrecognized command found at '^' position.
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface gi 0/0/0
[R1-GigabitEthernet0/0/0]ip address 192.168.1.1 24
May 4 2022 10:06:50-08:00 R1 %%01IFNET/4/LINK_STATE(1)[0]:The line protocol IP
on the interface GigabitEthernet0/0/0 has entered the UP state.
[R1-GigabitEthernet0/0/0]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R1]ip pool net1
Info: It's successful to create an IP address pool.
[R1-ip-pool-net1]network 192.168.1.0 mask 255.255.255.0
[R1-ip-pool-net1]gateway-list 192.168.1.1
[R1-ip-pool-net1]dns-list 192.168.1.1 114.114.114.114
[R1-ip-pool-net1]display this
[V200R003C00]
#
ip pool net1
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
 dns-list 192.168.1.1 114.114.114.114
#
return
[R1-ip-pool-net1]interface gi 0/0/0
[R1-GigabitEthernet0/0/0]dhcp select global
[R1-GigabitEthernet0/0/0]save
```

在主机 A、B 端使用 ipconfig 命令测试 DHCP 服务的工作情况，经检验发现路由器可以正确分配 192.168.1.0 网段的 ip 地址，主机 A、B 互相可以 ping 通。

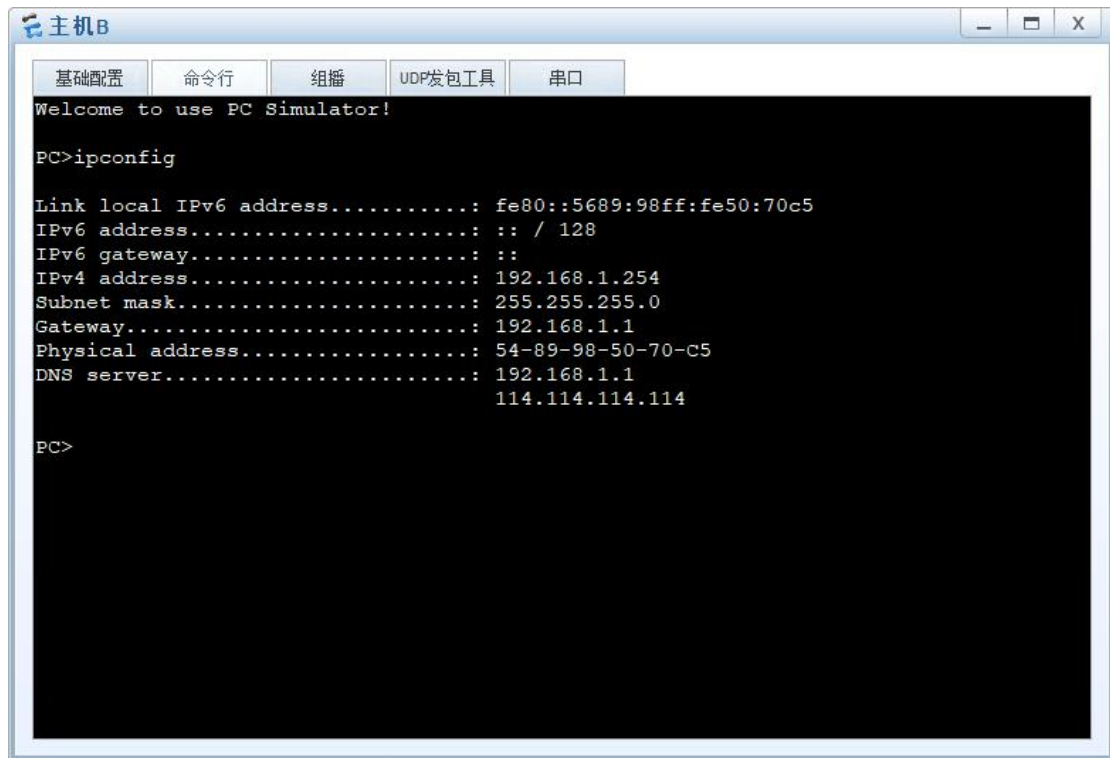


```
主机A
Welcome to use PC Simulator!

PC>ipconfig

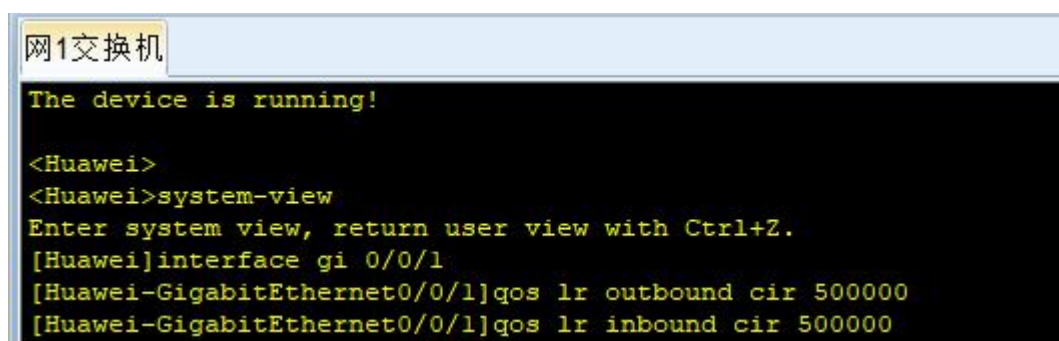
Link local IPv6 address.....: fe80::5689:98ff:fe0f:6a73
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.1.253
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.1.1
Physical address.....: 54-89-98-0F-6A-73
DNS server.....: 192.168.1.1
                  114.114.114.114

PC>
```



QoS 限速功能的配置:

根据实验要求, 对交换机 1 的 Ge 0/0/1 接口进行 QoS 限速, 根据设备情况可知, Ge 端口为千兆以太网接口, 故得出 Ge 0/0/1 口进行 50% 端口限速的限制速率为 500Mbps, 故使用 qos lr 命令将端口的上行下行速率均限制为 500Mbps, 并通过 Display current-configuration 命令和发包测试检查限速效果, 发现限速结果符合预期。



ARP 泛洪攻击的防范措施:

(1) 基于源 IP 地址进行时间戳抑制

这一方案的理念是控制某一个 IP 地址每秒发送的 ARP 报文数量(实验中设置为 50)。

超过该限制的报文将被丢弃。

由于 C, D 两个主机是静态 IP 地址, 故对这两台主机实施此方案。

命令设置在交换机上 (即交换机 2,3)

以计算机 D 的配置为例, 具体命令如下:

```
arp speed-limit source-ip 192.168.3.4 maximum 50
```

在交换机三输入: display current-configuration, 可以看到如下配置结果:

```
#  
arp speed-limit source-ip 192.168.3.4 maximum 50
```

(2) 配置 ARP 端口级防护

这一方案的思路是在各个接口配置 ARP 报文通过的速率, 如果 ARP 报文超出该速率, 将会在 1 秒内持续丢弃 ARP 报文。

此策略设置在交换机各个接口上。

以交换机一 gi 0/0/1 端口为例

实验中设置为每秒 50 个 ARP 报文的上限。

具体命令为:

```
arp anti-attack rate-limit enable
```

```
arp anti-attack rate-limit 50
```

display结果如下:

```
interface GigabitEthernet0/0/1  
  qos lr outbound cir 500000 cbs 62500000  
  qos lr inbound cir 500000 cbs 62500000  
  arp anti-attack rate-limit enable  
  arp anti-attack rate-limit 50 1  
#
```

ARP 欺骗的防范措施:

(1) ARP 表项固化

我们可以在网关第一次学习 ARP 表项时将其固化, 以防攻击者的恶意报文在之后使

得网关错误学习。

因为 A,B 两台计算机由 DHCP 获取 IP，我们在路由器二进行全局 ARP 表固化。

具体命令为：

arp anti-attack entry-check fixed-mac enable

此处的 fixed-mac 模式意味着用户 MAC 地址固定，但用户接入位置频繁变动的场景。当用户从不同接口接入交换机时，交换机上该用户对应的 ARP 表项中的接口信息可以及时更新。

在路由器二输入：display current-configuration，可以看到如下配置结果：

```
#
arp anti-attack entry-check fixed-mac enable
#
```

(2) ARP 报文内 MAC 地址一致性检查

这一防范措施的意义在于对 ARP 报文的源 MAC 地址和以太网帧头部的源 MAC 地址进行一致性检查。因为以太网帧头部的 MAC 地址是自动生成的，本身不可欺骗。故由此可以拦截欺骗性报文。

这一方案配置在各个交换机上，全局配置。

命令为：

arp anti-attack packet-check sender-mac

display 结果如下：

```
#
arp anti-attack packet-check sender-mac
#
```

四、评价标准

	项目	满分
设计与实验报告	方案(含测试方案)设计与论证	10
	结果与分析	10
	报告的完整性和规范性	10
	小计	30

实验内容	完成实验环境搭建	20
	DHCP 服务配置正确	5
	主机 C 与主机 D 网络参数配置正确	5
	任意两台主机之间路由可达	10
	限速功能配置正确	10
	网络安全功能配置正确	20
	小计	70
	合计	100