实验报告

课程名称： 网络交换技术

年级、专业： 2022级通信工程

姓名： 何予琦

学号： 20221060041

任课教师：杨俊东

成绩：

日期： 2025年 04 月 13日

**云南大学信息学院**

1. **实验目的**

（1）DHCP实验

掌握路由器DHCP服务器的配置方法

掌握DHCP中继代理的配置方法

掌握DHCP协议及其中继的原理及实现过程

1. NAT实验

掌握NAT网络地址转换的原理及功能

掌握NAT地址映射和端口映射的配置方法

掌握广域网(WAN)接入技术的原理

1. **实验设备**

仿真软件cisco packet tracer

1. **实验原理**
2. DHCP实验

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议，使用UDP协议工作， 主要有两个用途：给内部网络或网络服务供应商自动分配IP地址，给用户或者内部网络管理员作为对所有计算机作中央管理的手段。

当DHCP客户机Client与DHCP服务器Server在同一个物理网段，则客户机可以正确地获得动态分配的ip地址。DHCP的实现过程，大致如下：

客户机请求DHCP：首先向局域网内广播DHCP Discover包（源地址为0.0.0.0，目的地址为255.255.255.255），找到能够给它提供IP的DHCP服务器。

服务器响应：当可用的DHCP Server接收到Discover包后，通过发送DHCP Offer包给予应答，意在告诉Client端它可以提供IP地址。

客户机请求IP：Client端接收到Offer包之后，发送DHCP Request包请求分配IP。

服务器确认IP租约：DHCP Server发送ACK数据包，确认信息。

DHCP中继(代理)，即DHCP Relay（DHCPR），可以实现在物理网段和不同子网之间处理和转发dhcp信息的功能。如果不在同一个物理网段，则需要中继代理。DHCP中继的实现过程，大致如下：

当客户机启动并进行DHCP初始化时，它会在本地网络广播配置请求报文。

如果本地网络存在DHCP服务器，则可以直接进行DHCP配置，不需要DHCP中继。

如果本地网络没有DHCP服务器，则本地网络中的DHCP代理收到该广播报文后，将该DHCP报文的源IP地址修改为该Vlanif或上联接口的IP地址，而目的地址则为DHCP代理配置的DHCP服务器IP地址，以单播形式将DHCP Discovery包转发给指定DHCP服务器。

DHCP服务器根据请求信息进行配置，并直接转发给DHCP中继，再将配置信息以广播形式发送给客户机，完成IP地址动态分配。

1. NAT实验

在互联网中，公有地址用于不同外网之间通信，全球唯一并且能在公网上被路由；而私有地址用于网络内部，对于不同内网，私有地址可重用，但私有地址无法实现不同”外网-内网“或"内网-内网"之间通信，因为私有地址不能被路由。它要与外网通信，必须经过NAT设备（如网关，路由器）。

网络地址转换(NAT,Network Address Translation)属于接入广域网(WAN)技术，是一种将私有IP地址转化为公有IP地址的转换技术，主要用于实现内部网络主机访问外部网络的功能。根据转换方式有基于地址映射（三层技术，双向通信）和基于地址端口映射（四层技术，单向通信）两种，常见NAT类型包括：

静态NAT：将私网中的主机地址永久地、映射为公网中的固定合法IP地址（一对一）。

动态NAT：通过定义一系列的合法公有地址池，将每个内部本地地址动态地、一一映射为合法的内部全局地址。

NAPT：将多个内部地址都映射到一个合法公网地址(外网接口或公有地址池)，以不同的协议端口号与不同的内部地址相对应（多对一）。

端口映射：通过静态配置，将私网中的主机地址及端口映射为一个固定的公有地址及端口（一对一）。

根据NAT模型定义，可将路由器所连接的网络分别视为内部网络（内网）和外部网络（外网）。注意"内网与外网"，"私网与公网"的区别；

内部地址和外部地址：分别对应于NAT定义的内部网络和外部网络的所有地址；

本地地址：出现在“某个网络”内部的所有地址，包括内部本地地址(Inside Local)和外部本地地址(Inside Global)；

全局地址：出现在“某个网络”外部的所有地址，包括内部全局地址(Outside Local)和外部全局地址(Outside Global)；

NAT设备在公网和私网之间扮演代理的角色，其特点有：

NAT网关设置在私网到公网的路由出口位置，双向流量必须都要经过NAT网关；

网络访问只能先由私网侧发起，公网无法主动访问私网主机；

NAT网关在两个访问方向上完成两次地址的转换或翻译，出方向做源信息替换，入方向做目的信息替换；

NAT网关的存在对通信双方是保持透明的；

NAT网关为了实现双向翻译的功能，需要维护一张关联表，把会话的信息保存下来

与一般NAT不同，NAPT采用TCP端口多路复用方式，通过不同的协议端口号与不同的内部地址一一对应提供并发性，内网所有主机均可共享一个公有IP地址以实现对Internet的访问。NAPT能最大限度地节约IP地址资源，同时可隐藏内网主机，有效避免来自外网的攻击，因此被广泛应用于各种类型Internet接入方式和各种类型的网络中，是最常用的NAT类型。

NAPT也称“多对一”的NAT、端口地址转换(Port Address Translations, PAT)、地址重载(Address Overloading)

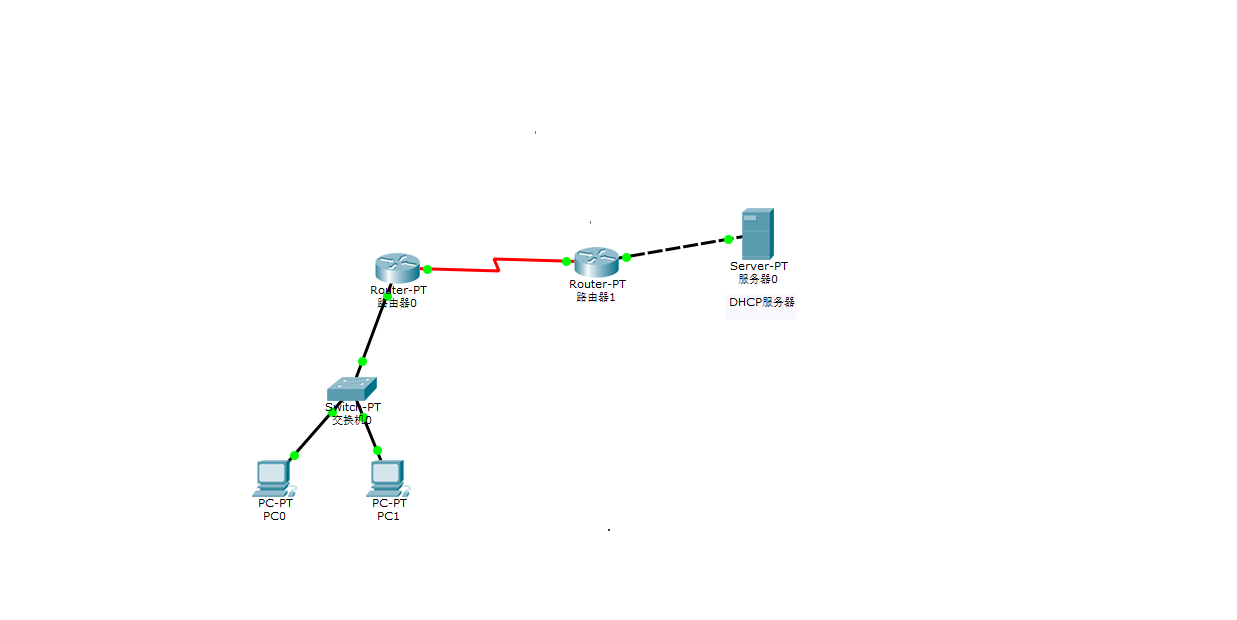
与动态NAT的区别：NAPT相当于“开启了地址重载的动态NAT”，扩展了对TCP和UDP的端口号的转换

优势：能够使用一个全球有效IP地址获得通用性

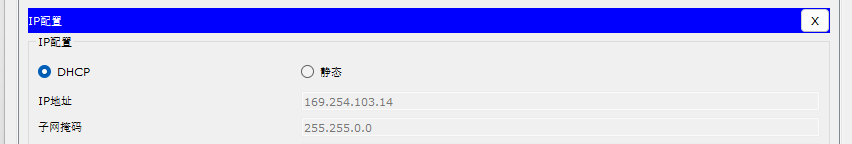
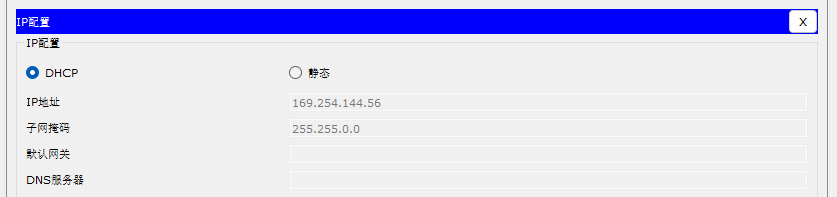
缺点：其通信仅限于TCP或UDP协议

1. **实验结果记录与分析**

1、DHCP实验



**DHCP实验网络拓扑图**



成功获得ip地址

DHCP服务器配置（以Router0为例）

启用DHCP服务功能

Router(config)#service dhcp

启用路由器的DHCP功能，使其具备分配IP地址的能力。

配置DHCP地址池 cisco1

Router(config)#ip dhcp pool cisco1

Router(dhcp-config)#network 192.168.1.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.1.1

Router(dhcp-config)#dns-server 114.114.114.114

Router(dhcp-config)#exit

定义地址池名称为 cisco1，为子网 192.168.1.0/24 分配IP地址。设置的默认网关是 192.168.1.1，DNS服务器地址为 114.114.114.114。

排除静态IP地址段

Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.100

该命令排除地址段 192.168.1.1 到 192.168.1.100，这些IP将不会被DHCP动态分配，通常用于服务器或网关等设备的静态地址。

配置第二个DHCP地址池 cisco2（用于Router1网络）

Router(config)#ip dhcp pool cisco2

Router(dhcp-config)#network 192.168.2.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.2.1

Router(dhcp-config)#dns-server 114.114.114.114

Router(dhcp-config)#exit

为另一个子网 192.168.2.0/24 配置地址池，默认网关设置为 192.168.2.1，DNS服务器同样为 114.114.114.114。

排除第二子网的静态IP

Router(config)#ip dhcp excluded-address 192.168.2.100 192.168.2.200

为避免冲突，排除地址段 192.168.2.100 到 192.168.2.200。

二、DHCP中继代理配置（在Router1中配置）

启用DHCP服务

Router(config)#service dhcp

设置中继地址

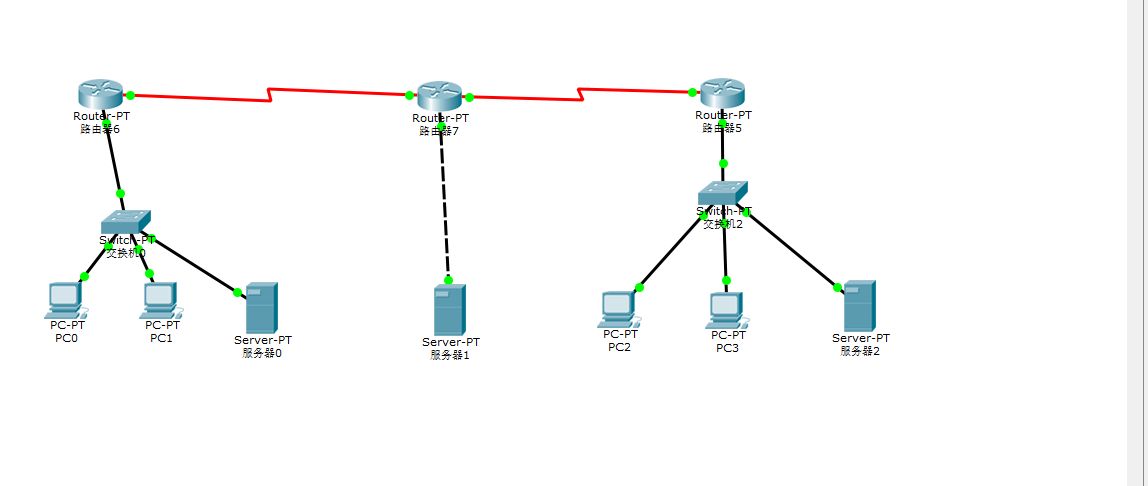
Router(config)#interface f0/0

Router(config-if)#ip helper-address 10.254.10.1

在Router1的FastEthernet 0/0接口上启用DHCP中继功能，使用 ip helper-address 命令将子网 192.168.2.0 中的DHCP请求转发到Router0的 10.254.10.1 接口，实现跨子网的DHCP服务。

通过配置Router0为DHCP服务器并在Router1上设置中继转发，使两个不同子网的终端都能自动获取IP地址。本实验体现了DHCP集中式地址管理的优势，并展示了跨子网部署的基本方法，提升了网络自动化管理水平。

2、NAT实验



**NAT实验网络拓扑图**

1. 静态NAT配置

静态NAT用于将内部私有IP地址映射到一个固定的公共IP地址。

步骤：

配置内部接口 (f0/0) 和外部接口 (s2/0)：

R0(config)#inter f0/0

R0(config-if)#ip nat inside

R0(config-if)#exit

R0(config)#inter s2/0

R0(config-if)#ip nat outside

R0(config-if)#exit

这里将 f0/0 接口定义为内部接口（ip nat inside），s2/0 接口定义为外部接口（ip nat outside）。

配置静态NAT映射：

R0(config)#ip nat inside source static 192.168.1.100 12.1.1.5

将内部IP 192.168.1.100 映射到公共IP 12.1.1.5，实现固定映射。

2. 动态NAT配置

动态NAT用于动态分配公共IP地址池，并通过访问控制列表（ACL）来决定哪些内部IP地址可以进行映射。

步骤：

创建公共IP地址池：

R0(config)#ip nat pool no-pat 12.1.1.1 12.1.1.3 netmask 255.255.255.0

创建了一个包含 12.1.1.1 到 12.1.1.3 范围的公共IP地址池。

配置访问控制列表（ACL），指定哪些内部网络IP可以进行NAT映射：

R0(config)#access-list 7 permit 192.168.1.0 0.0.0.255

该访问控制列表允许IP地址范围 192.168.1.0/24 进行映射。

将内部网络和公共地址池关联：

R0(config)#ip nat inside source list 7 pool no-pat

这条命令将访问列表 7 与 no-pat 地址池关联，允许从 192.168.1.0/24 范围的内部网络地址进行NAT。

3. 端口映射（NAPT配置）

NAPT是动态NAT的一种扩展，它可以让多个内部设备共享一个公共IP地址，通过映射不同的端口号来区分不同的流量。

步骤：

创建访问控制列表，指定哪些内部网络IP可以进行端口映射：

R2(config)#access-list 5 permit 172.16.1.0 0.0.0.255

该访问控制列表允许 172.16.1.0/24 范围内的设备进行NAT。

配置NAT地址重载（PAT）：

R2(config)#ip nat inside source list 5 interface Serial2/0 overload

这条命令将访问列表 5 与 Serial2/0 接口的外部IP地址关联，启用地址重载（PAT），使多个内部设备共享一个公共IP地址。

配置静态端口映射，将Server2的内网80端口映射到外网接口IP的80端口：

R2(config)#ip nat inside source static tcp 172.16.1.100 80 23.1.1.1 80

1. **问题、收获与建议**

1、DHCP实验

通过本次实验，我掌握了在Cisco路由器上配置DHCP服务器的基本方法，能够完成地址池的创建、默认网关和DNS服务器的设置以及地址排除操作。同时，我理解了DHCP中继代理的工作原理，并成功实现了跨子网的动态地址分配。实验进一步加深了我对网络自动化管理和动态路由配置的理解，提升了实际动手能力和故障排查能力。

2、NAT实验

通过本次实验，我深入了解了NAT（网络地址转换）的原理及其在路由器中的配置应用。具体收获如下：

静态NAT与动态NAT的区别：我掌握了静态NAT的固定映射机制，即内部私有IP地址与公共IP地址一一对应。而动态NAT则使用地址池，根据实际需要动态分配公共IP，适合需要多个设备访问外网的情况。

端口映射与NAPT的理解：通过配置端口映射（NAPT），我理解了如何通过共享一个公共IP地址，利用不同的端口区分不同的内部设备。这对于节省IP地址资源非常有效，尤其是在IP地址有限的情况下。

ACL与NAT结合的应用：配置访问控制列表（ACL）对NAT的应用让我更加清楚地理解了如何限制哪些内部网络可以进行NAT映射。这为网络安全管理提供了灵活性，能够精确控制哪些设备可以访问外部网络。

路由器接口配置：通过对路由器接口（如f0/0、s2/0）的配置，我掌握了如何定义内外网接口，并应用不同的NAT策略，确保数据流的正确转发和转换。