



西安电子科技大学
XIDIAN UNIVERSITY

数据网络综合设计实验 实验报告

目录

1	实验目的	1
2	实验仪器	1
3	实验原理	1
3.1	局域网的拓扑结构	1
3.2	虚拟局域网 VLAN	1
3.2.1	概述	1
3.2.2	工作原理	2
3.2.3	标准	3
3.2.4	应用	3
3.3	路由	3
3.3.1	路由器的定义和作用	3
3.3.2	基本概念	4
3.3.3	路由器的工作原理	6
3.3.4	IP 路由过程	6
3.3.5	路由器与二层交换机互联的配置方法	7
3.3.6	路由器的配置	8
3.3.7	子接口的定义	8
3.4	DHCP 技术	9
3.4.1	简介	9
3.4.2	特性	9
3.4.3	分配方式	9
3.4.4	工作原理	9
3.5	NAT 技术	10
3.5.1	简介	10
3.5.2	关键概念	10
3.5.3	工作原理	11
3.5.4	测试结果	11
3.6	GRE 隧道技术	11
3.6.1	简介	11
3.7	ACL 技术	12
3.7.1	简介	12
3.7.2	工作原理	12
3.7.3	测试结果	12
4	实验要求	12

5	实验步骤	13
5.1	绘制拓扑结构	13
5.2	搭建网络	13
5.3	配置 VLAN	14
5.4	配置交换机端口	14
5.5	配置路由器端口	15
5.6	配置 DHCP	17
5.7	配置 NAT	19
5.8	配置路由表	20
5.9	配置 GRE 隧道	22
5.10	测试网络	23
6	心得体会	24

数据网络综合设计实验 实验报告

1 实验目的

1. 了解局域网中的基本概念及基本命令；
2. 了解 VLAN 的概念及作用，了解交换机的 VLAN 接口类型并学习配置交换机的 VLAN；
3. 学习使用 DHCP 技术为网络中的设备动态分配 IP 地址；
4. 学习使用 NAT 技术完成本地网络和公共网络之间的地址变换；
5. 掌握交换机和路由器的互连方法；
6. 学习利用单臂路由完成网络中设备的互连；
7. 学习使用 GRE 隧道技术连接网络中的设备；
8. 学习使用 ACL 技术控制设备的访问；

2 实验仪器

1. 电脑；
2. Cisco Packet Tracer 5.0 软件。

3 实验原理

3.1 局域网的拓扑结构

局域网是由多个交换设备，按照一定的拓扑结构相互连接而成的，常用的拓扑结构有星型结构、环型结构、总线型结构和树型结构。

3.2 虚拟局域网 VLAN

3.2.1 概述

虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的技术。划分 VLAN 的主要作用是隔离广播域，如图 1 所示。广播域，指的是广播帧（目标 MAC 地址全部为 1）所能传递到的范围，亦即能够直接通信的范围。严格地说，并不仅仅是广播帧，多播帧（Multicast Frame）和目标不明的单播帧（Unknown Unicast Frame）也能在同一个广播域中畅行无阻。本来，二层交换机只能构建单一的广播域，不过使用 VLAN 功能后，它能够将网络分割成多个广播域。

如果仅有一个广播域，有可能会影响到网络整体的传输性能。

如果整个网络只有一个广播域，那么一旦发出广播信息，就会传遍整个网络，并且对网络中的主机带来额外的负担。因此，在设计 LAN 时，需要注意如何才能有效地分割广播域。

分割广播域时，一般要使用路由器，以路由器上的网络接口（LAN Interface）为单位分割广播域。但是，通常情况下路由器上不会有太多的网络接口，其数目多在 1-4 个左右。随着宽带连接的普及，宽带路由器（或者叫 IP 共享器）变得较为常见，但是需要注意的是，它们上面虽然带着多个（一般为 4 个左右）连接 LAN 一侧的网络接口，但那实际上是路由器内置的交换机，并不能分割广播域。况且使用路由器分

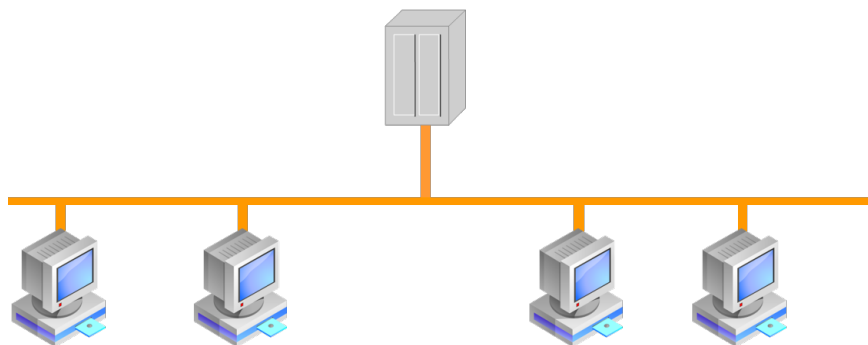


图 1: 广播域

割广播域的话，所能分割的个数完全取决于路由器的网络接口个数，使得用户无法自由地根据实际需要分割广播域。

与路由器相比，二层交换机一般带有多个网络接口。因此如果能使用它分割广播域，那么无疑运用上的灵活性会大大提高。用于在二层交换机上分割广播域的技术，就是 VLAN。通过利用 VLAN，我们可以自由设计广播域的构成，提高网络设计的自由度。

3.2.2 工作原理

如图 2 所示，在进行跨交换机 VLAN 通信时，需要一个端口将不同交换机的报文进行交换。这里需要这个端口具有一个特点，那就是可以工作在不同的 VLAN 之中，这样子可以减少资源的损耗，提高通信效率。

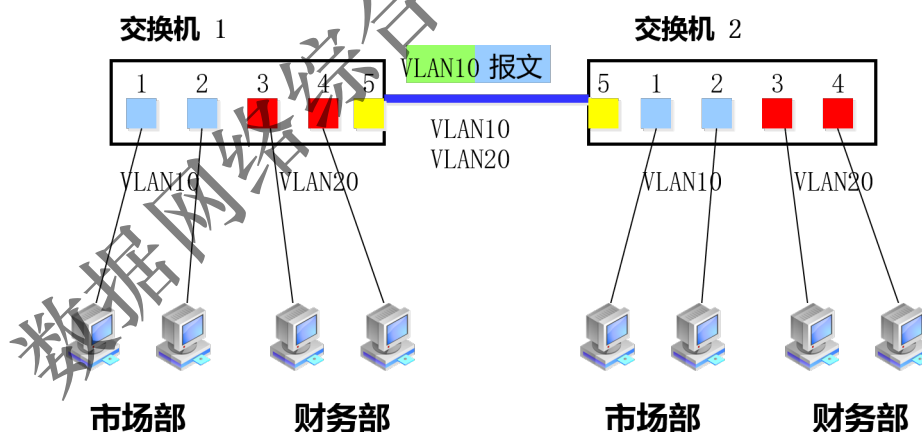


图 2: 跨交换机 VLAN 工作

如图 3 所示，报文分为两种类型，带标签的报文（tag）和不带标签的报文（untag）。前者由 MAC 地址、IP 地址和数据部分组成，后者则增加了 VLAN 标识，标注 VLAN 编号。这两种报文就应用在下面描述的不同端口当中。

交换机的端口，可以分为两种：访问连接（Access Link）和汇聚连接（Trunk Link）。

访问连接（Access Link）指的是只属于一个 VLAN，且仅向该 VLAN 转发数据帧的端口，由于不用区分不同的 VLAN 编号，这种端口发送不带标签的报文，一般与 PC 或 Server 相连接时使用。

汇聚连接（Trunk Link）指的是让交换机互联的网线集中到一根上，能够转发多个不同 VLAN 的通信的端口，由于需要区分不同 VLAN，在汇聚连接发送的报文中，需要携带标签，标注 VLAN 编号，一般用于交换机级联端口传递多组 VLAN 信息。

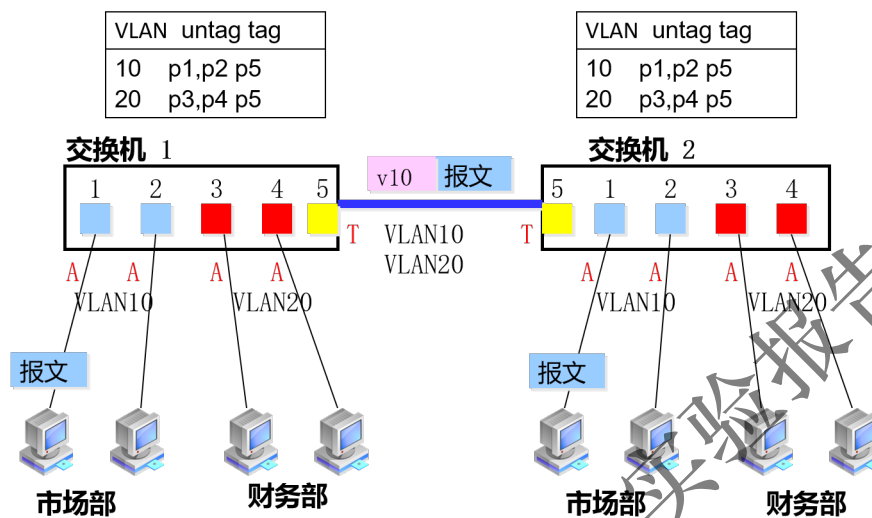


图 3: 携带标签和不携带标签的报文

交换机在接收报文时需要判断报文在哪个 VLAN 中转发。如果接收到 tag 报文，就按照 tag 中标注的 VID 中转发，如果接收到 untag 报文，就按照接收端口所在的 VLAN 转发。而交换机发送报文时，是否携带标签，需要通过发送端口的 VLAN 属性判断，Access 端口发送 untag 报文，Trunk 端口发送 tag 报文。

3.2.3 标准

VLAN 中不同的端口，有不同的标准。

访问端口（Access Port）发送不带标签的报文（untag），一个访问端口只属于一个 VLAN，缺省所有端口都包含在 VLAN1 中，并且都是访问端口。

汇聚端口（Trunk Port）通过发送带标签的报文（tag）来区别某一数据表属于哪一 VLAN，一个汇聚端口可以属于多个 VLAN，标签遵从 IEEE802.1Q 协议标准。

3.2.4 应用

宽带小区中要求每一个用户都能够与外网通信，但用户之间不能互通，防止其中一用户出现网络问题（如中病毒）其他用户也一起受影响。

3.3 路由

3.3.1 路由器的定义和作用

路由器是用于网络互连的计算机设备，其核心作用是实现网络互连，数据转发。

其作用具体体现为：

1. 路由（寻径），即路由表建立、刷新；

2. 交换，在网络之间转发分组数据；
3. 隔离广播，指定访问规则；
4. 异种网络互连。

3.3.2 基本概念

1. 路由表

路由器为执行数据转发路径选择所需要的信息被包含在路由器的一个表项中，称为“路由表”。当路由器检查到包的目的 IP 地址时，它就可以根据路由表的内容决定包应该转发到哪个下一跳地址上去。路由表被存放在路由器的 RAM 上。

2. 路由表的构成

路由表由目的网络地址（Dest）、掩码（Mask）、下一跳地址（Gw）、发送的物理端口（Interface）、路由信息的来源（Owner）、路由优先级（Pri）、度量值（Metric）构成。

网络地址和掩码相与的结果用于定义本地计算机可以到达的目的网络的范围。通常情况下，网络目的地址方为包含以下四种：

1. 主机地址：某个特定主机的网络地址；
2. 子网地址：某个特定的子网的网络地址；
3. 网络地址：某个特定网络的网络地址；
4. 默认路由：所有未在路由表中指定的网络地址。

网关又称为下一跳服务器，在发送 IP 数据包时，网关定义了针对特定网络目的地址，数据包发送到下一跳服务器。如果是本地计算机直接连接到的网络，网关通常是本地计算机对应的网络接口，但是此时接口必须和网关保持一致；如果是远程网络或默认路由，网关通常是本地计算机所连接到网络上的某个服务器或路由。

接口定义了针对特定的网络目的地址，本地计算机用于发送数据包的网络接口。网关必须位于和接口相同的子网（默认网关除外），否则会造成在使用此路由项时调用其他路由项，从而导致路由死锁。

度量值又称为跃点数，用于指出路由的成本，通常情况下代表到达目标地址所需要经过的跃点数量，一个跃点代表经历一个路由器。跃点数越低，代表路由成本越低，跃点数越高，代表路由成本越高。当具有多条到达相同目的网络的路由项时，TCP/IP 会选择具有更低跃点数的路由项。

本次实验主要研究网络地址和下一跳地址。

3. 路由表的建立和维护

1) 静态路由表

由系统管理员事先设置好的固定路由表称为静态路由表，静态路由表是在安装系统的时候就根据网络配置情况预先设定的，不会随着未来网络结构的改变而改变。

2) 动态路由表

动态路由表是由路由器根据网络系统的运行状况而自动调整形成的路由表。路由器根据路由选择协议提供的功能，自动学习和记忆网络运行状况，在需要时自动选择数据传输的最佳路径。

路由表需要一个建立过程，也就是初始化路由表，不同的网络操作系统有不同的初始化方式，大体来说常见的有三种：

1) 路由器启动时, 从外部读入一个完整的寻径表, 储存在内存中, 系统关闭时再将当前路由表 (可能经过刷新) 写回外存, 供下次使用;

2) 系统启动时, 只提供一个空表, 通过执行显式指令, 如批处理文件中的指令, 来填充;

3) 系统启动时, 从与本路由器直接相连的各网络地址中, 推导出一组初始路由, 通过初始路由只能访问相连网上的主机。

很显然, 无论哪种情况, 初识路由表总是不完善的, 需要不断地运行过程加以补充, 这就是路由表的刷新。

路由器自动获取路径信息的有两种方法, 向量-距离算法和链路-状态算法。

1) 向量-距离算法

向量-距离 (Vector-Distance, 简称 VD) 算法, 它的基本思想是: 路由器周期性的向与其相邻的路由器广播刷新报文, 报文的主要内容是一组从本路由器出发去往信宿网络的最短距离 (路由器进行路由选择的原理是最短路径优先原则), 各个路由器根据收到的 (V,D) 报文, 按照最短路径优先原则对各自的路由表进行刷新。该算法的路径刷新发生在相邻网关之间, 所以 (V,D) 不一定以广播的形式发送, 也可以是组播或者是一对一的发送。(V,D) 报文中的 V 代表 “向量”, 标识从该路由器可以到达的网络或者是主机; D 代表距离, 表示从该路由器到信宿 V 的跳数。

值得注意的是, 该算法虽然简单, 易于实现, 但是它的信息交换量大, 当交换路由信息的时候, 几乎传输整个路由表, 收敛速度慢。所谓的收敛速度慢就是当网络发生变化的时候, 路由器不能及时的检测到这种情况, 因为变化的扩散和传输需要一定的时间, 而其他的路由器在没有获取到这种变化是不能正确的反应网络拓扑的真实情况的。所以该算法不适合那些网络结构频繁变化的或者大型的网络结构。

2) 链路-状态算法

链路-状态 (Link-Status, 简称 L-S) 算法, 也叫最短路径优先 (Shortest Path First, 简称 SPF) 算法, 它的主要做法如下:

a. 首先由路由器向相邻路由器发送查询报文, 测试和它相邻路由器的链路状态。如果可以收到相邻路由器发回的响应, 则说明该相邻路由器和这个路由器之间可以正常通信;

b. 在收到该路由器和其他相邻路由器的链路状态后, 向系统中所有参加最短路径优先算法的路由器发送链路状态报文;

c. 各路由器收到其他路由器发来的链路状态报文后, 根据报文中的数据刷新本路由器所保存的网络拓扑结构图。如果链路发生变化, 路由器将启用 Dijkstra 算法生成新的最短路径优先数, 并刷新本地路由表。

4. 路由分类

1) 直连路由

当接口配置了网络协议地址并状态正常时, 接口上配置的网段地址自动出现在路由表中并与接口关联, 并随接口的状态变化在路由表中自动出现或消失。

2) 静态路由

这是单向路由, 还需要在对方的路由器上配置一条相反的路由。

3.3.3 路由器的工作原理

最重要的是路由功能和交换/转发功能。

1. 路由功能

学习和维护网络拓扑结构知识的机制，产生和维护路由表。

2. 交换/转发功能

如图 4所示，数据在路由器内部移动与处理的过程（数据从路由器一个接口输入，然后选择合适接口输出、做帧的解封装与封装，并对包做相应处理）。

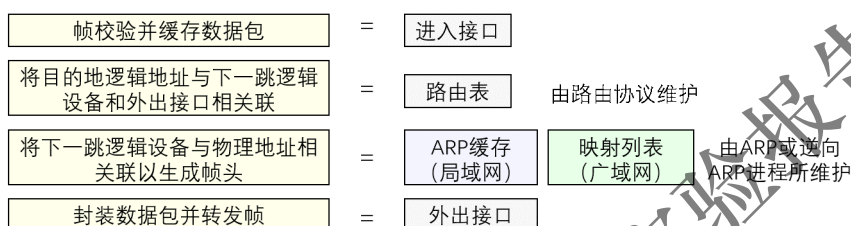


图 4: 交换/转发功能

3.3.4 IP 路由过程

图 5给出了 IP 路由过程的流程图。

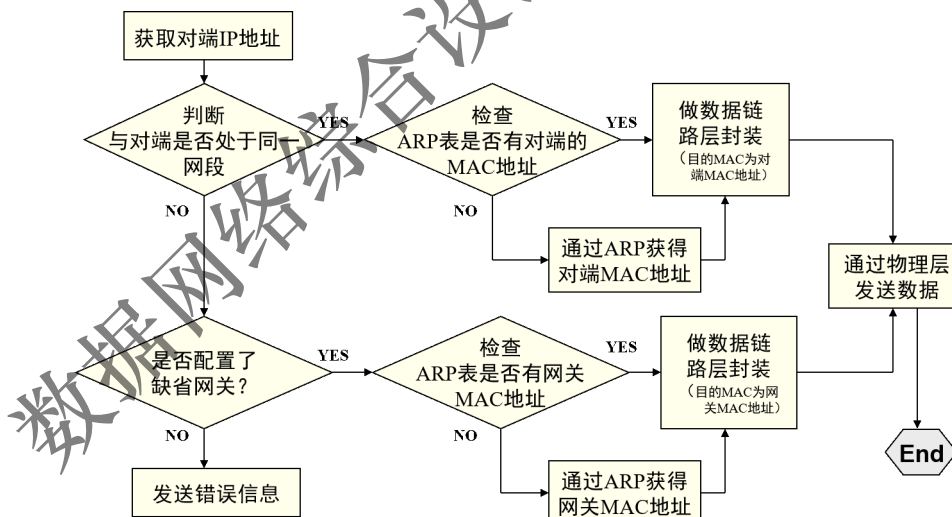


图 5: IP 路由过程

1. 同一网络内部的通信

图 6给出了同一网络内部通信过程中，网络情况和协议层次结构。

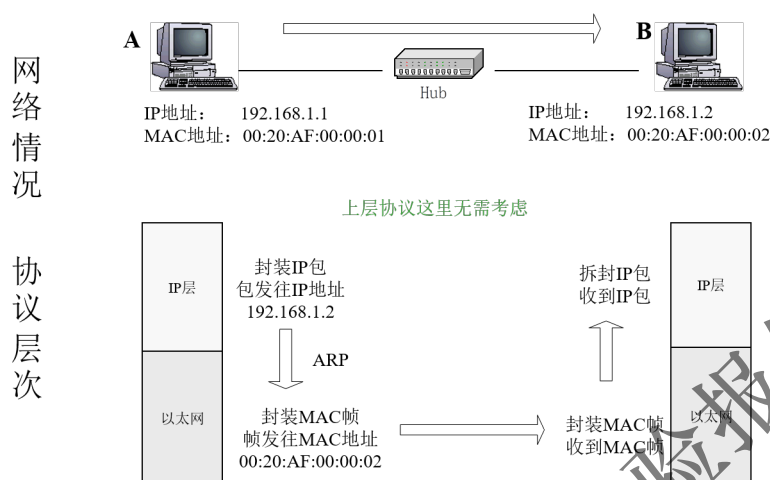


图 6: 同一网络内部通信过程

2. 不同网络之间的通信

图 7给出了不同网络之间的通信过程中，网络情况和协议层次结构。

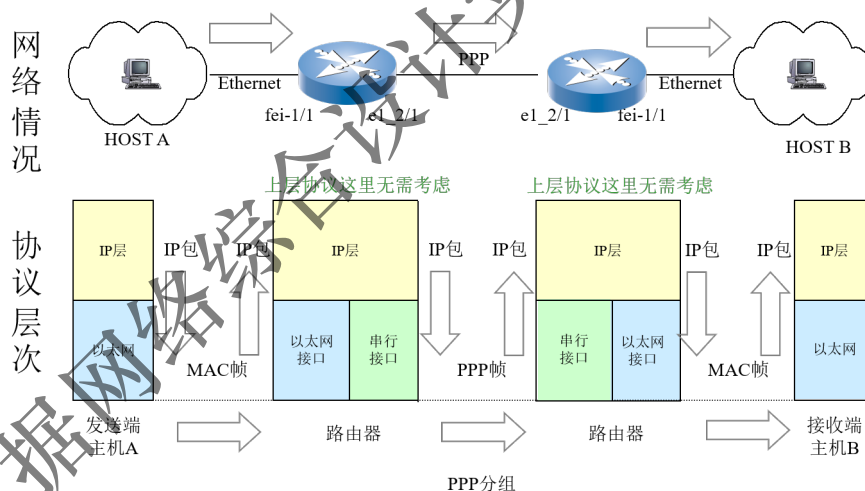


图 7: 不同网络之间通信过程

3. IP 通信流程基本概念

IP 通讯是基于 hop by hop 的方式，从源到目的之间源 IP 和目的 IP 地址保持不变，每经过一个数据链路层，数据链路层封装都要做相应的重新封装，返回的数据选路与到达的数据选路无关。

3.3.5 路由器与二层交换机互联的配置方法

连接如图 8, ROUTE 的 F1/0 与 SWITCH 的 F0/0 相连, SWITCH 的 F0/1、F0/2、F0/3 分别与 PC1、PC2、PC3 相连接, PC1 分到 VLAN10, PC2、PC3 分到 VLAN20。

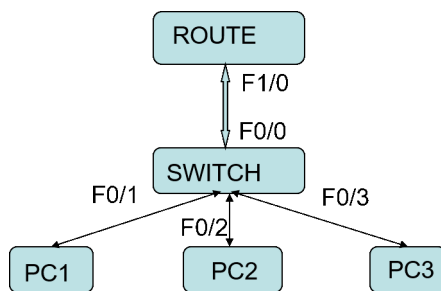


图 8: 路由器与二层交换机互联图示

3.3.6 路由器的配置

二层交换机的 Trunk 端口与路由器子接口配合，一个路由器物理接口内的每个子接口对应交换机的一个 VLAN，通过路由器内部子接口之间第三层包的相互转发，实现 VLAN 之间的第三层互通，是此类组网的目的。而二层交换机没有路由功能，无法实现多个 VLAN 之间的第三层互通。

在此类组网中，路由器以太网子接口在一个 VLAN 中充当网关的作用。在配置时，其 IP 地址的子网地址一定要正确，属于同一个 VLAN 的交换机各端口上的 PC 机的默认网关应该设置为该子接口的 IP 地址。

```
1 Router(config-subif)#encapsulation dot1q 10
```

注意，在子接口先要描述 DOT1Q，再配 IP 地址，DOT1Q 后面的数字是 VLAN 的号码，根据交换机的配置不同有所不同。

3.3.7 子接口的定义

所谓子接口，就是在一个物理接口上配置出来的多个逻辑上的虚接口。这些虚接口共用物理接口的物理层参数，又可以分别配置各自的链路层和网络层的参数。因为这样的多个虚接口可以对应一个物理接口，故常被称为“子接口”。

```
1 Router(config)#int f0/0.1
2 Interface ethernet interface-number.subinterface-number
3 Undo Interface ethernet interface-number.subinterface-number
```

其中，interface-number 为接口编号，包括槽号、卡号、端口号。subinterface-number 为子接口编号，取值范围为 0 ~ 4096。在实际使用中，一个父接口可创建的子接口数目最大为 256。

```
1 Router>enable           //系统模式
2 Router#configure terminal //配置模式
3 Router(config)#int f0/0   //端口模式
4 Router(config-if)#no shut
5 Router(config)#EX
6 Router(config)#int f0/0.1
```

```

7 Router(config-subif)#encapsulation dot1q 10 //绑定VLAN10
8 Router(config-subif)#ip add 192.168.1.254 255.255.255.0
9 Router(config-subif)#exit
10 Router(config)#int f0/0.2
11 Router(config-subif)#encapsulation dot1q 20 //绑定VLAN20
12 Router(config-subif)#ip add 192.168.2.254 255.255.255.0
13 Router(config-subif)#exit
14 Router#copy run star //copy running-config startup-config 保存配置的简写

```

3.4 DHCP 技术

3.4.1 简介

DHCP 用来为网络中的设备动态分配 IP 地址，网关地址，DNS 服务器等网络配置参数。在大规模网络中手动地为所有的计算机配置 IP 地址的工作量简直无法想象，而且出错概率非常大，DHCP 使这个问题得到了很好的解决。

3.4.2 特性

1. 只需要保证 IP 地址和其他配置参数正确就能保证 DHCP 的正确运行，不需要检查每一台计算机；
2. 每一个 IP 地址只能同时租用给一个主机；
3. 计算机在不同子网移动的时候不需要重新设置 IP 地址；
4. 由服务器端和客户端两部分组成，服务器端为客户端提供分配 IP 地址的服务。

3.4.3 分配方式

1. 自动永久分配

一旦客户端向服务器端请求 IP 地址成功，那么它就可以永久的利用这个 IP 地址进行通信。

2. 自动租用分配

服务器端给客户端分配的 IP 地址是有期限的，一旦到达期限或者客户端放弃使用这个 IP 地址，这个 IP 地址就会回到 IP 地址池之中，等待下一次租赁。

3. 手动分配

客户端被分配的 IP 地址由网络管理员来事先选定，服务器端的工作就只剩下把这个已经选定的 IP 地址进行通告了。

3.4.4 工作原理

1.DHCP 发现（DHCP Discover）阶段

客户端首次被打开的时候会向整个网络上的所有 DHCP 服务器广播请求消息，请求一个可以被使用的 IP 地址。如果这个消息没有发送成功，客户端会在 5 分钟之后重复这个过程直到进入下个阶段。

2.DHCP 提供（DHCP Offer）阶段

当服务器端接受到请求消息的时候，它就会尝试在地址池里面寻找那些还没有被使用的 IP 地址，同时返回给客户端一个 DHCP Offer 消息，其中会含有一个使用期限。

当使用期限过了 1/2 的时候，客户端可以发送 DHCP Request 来请求延期使用当前 IP 地址；如果使用时间超过了 87.5%，客户端仍然没有向服务器端发送 DHCP Request 来请求延期，那么客户端就必须停止对当前 IP 地址的使用，假如客户端想要继续访问外网，那么就需要重新回到阶段一来重复这个过程。

3.DHCP 请求（DHCP Request）阶段

客户端通常会收到多个服务器端的 DHCP Offer，一般来说客户端会选择最先到达的那一个，然后向整个网络上广播一个 DHCP Request，通告其他服务器端它最终的选择是谁。和 DHCP Request 同时发送的还有一个 ARP 分组，用于验证在网络上是否存在另外的客户端正在使用这个 IP 地址来进行通信，假如得到肯定的结果，客户端就会发送 DHCP Decline 消息给客户端，来通告客户端它的 DHCP Offer 被拒绝了，并且重新回到阶段一来重复这个过程。

4.DHCP 确认（DHCP Ack）阶段

服务器端在接收到了 DHCP Request 之后，会给客户端返回一个 DHCP Ack，用来确认双方的 IP 地址租赁契约正式成立。

3.5 NAT 技术

3.5.1 简介

Internet 目前遇到的最迫切的挑战即是 IPv4 地址的严重匮乏和路由的可扩展性，虽然预见性的开发了 IPv6，但是把所有的地址都迁移到 IPv6 上是一个极度缓慢的过程，因此网络地址转换（NAT）的方案被广泛的采用。

NAT 的目标是解决私有网络如何访问公共网络的问题，后来人们想到任意两个网络之间数据传输时都可以采用这个方案来解决地址转换的问题。

NAT 的出现使多量私网 IP 映射成少量的公网 IP 成为可能，在一定程度上解决了 IPv4 地址空间的严重缺乏问题，同时也实现了对私网主机的隐私保护。

3.5.2 关键概念

1. 私网 IP 地址

不会在全球网络上被分配，所以可以在一个公司或者学校之类的自治系统内自由的使用。

2. 内部和外部

内部一般就是指内网，使用私网 IP；外部一般就是指 NAT 路由器所要访问的外网。

3. 静态 NAT

静态 NAT 的概念和静态路由的概念差不多，静态路由是固定路径，而静态 NAT 是固定配对。静态 NAT 可以实现外部公网和内网特定计算机的双工通信。

4. 动态 NAT

动态选择配对和映射方式。当内网的计算机请求和外网进行通信的时候，NAT 路由器就会从 IP 地址池中选择一个来和计算机形成配对映射。

5. 网络地址端口转换 (Network Address Port Translation, NAT)

NAPT, 它可以允许数个内网 IP 地址和同一个公网 IP 地址形成映射关系, 所以也被称为“多对一 NAT 地址转换”。它只需要一个公网 IP, 然后当内部计算机要求跟外网计算机进行通信的时候, 它会随机选择一个端口分配给内网计算机, 内网计算机通过这个端口来访问外网。NAPT 大大提升了效率和复用性, 因此被广泛的使用。

6. 地址转换控制

利用访问控制表 (Access Control Limit, ACL) 和 IP 地址池来控制地址转换。

3.5.3 工作原理

首先允许 192.168.66.0/24 网段允许访问外网, 设置公网 IP 的地址池为 202.7.7.20-202.7.7.70。

假设计算机 PC1 的 IP 地址为 192.168.66.1, 他想要访问的外网 IP 为 202.1.1.1, 这时 NAT 路由器会给 PC1 分配一个没有再被使用的公网 IP, 比如说是 202.7.7.27, PC1 的消息源地址是 192.168.1.7, 当这个消息通过 NAT 路由器的时候它的 IP 地址会被包装成 202.7.7.27, 这样就可以和外网进行通信了, 在外网 202.1.1.1 看来与它进行通信的就是 202.7.7.27 这个 IP, 当外网把信息传回来的时候, NAT 路由器就会按照映射关系, 把目的地址为 202.7.7.27 的信息转发给 192.168.66.1。

3.5.4 测试结果

1. 内网可以直接访问外网, 不需要路由;
2. 外网不能访问内网, 需要添加通过路由访问。

3.6 GRE 隧道技术

3.6.1 简介

GRE (Generic Routing Encapsulation, 通用路由封装) 协议是对某些网络层协议 (如 IP 和 IPX) 的数据报文进行封装, 使这些被封装的数据报文能够在另一个网络层协议 (如 IP) 中传输。GRE 采用了 Tunnel (隧道) 技术, 是 VPN (Virtual Private Network) 的第三层隧道协议。

Tunnel 是一个虚拟的点对点的连接, 提供了一条通路使封装的数据报文能够在这个通路上传输, 并且在一个 Tunnel 的两端分别对数据报进行封装及解封装。

一个 X 协议的报文要想穿越 IP 网络在 Tunnel 中传输, 必须要经过加封装与解封装两个过程, 下面以图 9 的网络为例说明这两个过程:



图 9: X 协议网络通过 GRE 隧道互连

1. 加封装过程

Router A 连接 Group 1 的接口收到 X 协议报文后, 首先交由 X 协议处理;

X 协议检查报文头中的目的地址域来确定如何路由此包；

若报文的目的地址要经过 Tunnel 才能到达，则设备将此报文发给相应的 Tunnel 接口；

Tunnel 口收到此报文后进行 GRE 封装，在封装 IP 报文头后，设备根据此 IP 包的目的地址及路由表对报文进行转发，从相应的网络接口发送出去。

2. 解封装的过程

解封装过程和加封装的过程相反。

Router B 从 Tunnel 接口收到 IP 报文，检查目的地址；

如果发现目的地是本路由器，则 Router B 剥掉此报文的 IP 报头，交给 GRE 协议处理（进行检验密钥、检查校验和及报文的序列号等）；

GRE 协议完成相应的处理后，剥掉 GRE 报头，再交由 X 协议对此数据报进行后续的转发处理。

3.7 ACL 技术

3.7.1 简介

ACL 可以实现信息识别功能，然后实现过滤，过滤的条件可以是消息的源地址、目的地址和端口号等。同时 ACL 的配置作为一种重要的安全控制技术，在实际的网络工程配置中经常会被使用到。基本上所有的路由协议都支持配置 ACL。

3.7.2 工作原理

消息在进来的时候会经历一次检查，第一次检查主要是判断这个消息是否能够路由，能路由就放行。紧接着路由器会根据 ACL 判断这个消息是否符合筛选条件，不符合就把它给丢弃。

消息在出去的时候也会经历一次检查，同样的，如果不符合 ACL 的筛选条件就被丢弃。

3.7.3 测试结果

1. 开启 ACL 可以访问其他节点；
2. 关闭 ACL 不能访问其他节点。

4 实验要求

按照搭建网络，实现：

1. 二层交换机的每个端口在不同 VLAN；
2. 利用静态路由来配置路由；
3. 要求用到 DHCP 技术来分配 IP 地址；
4. 要求用到 NAT 技术完成地址变换；
5. 要求用到单臂路由来实现互联；
6. 要求用到 GRE 隧道技术；
7. 要求用到访问控制列表技术；

8. 任意两个节点之间能在规则下互相访问。

5 实验步骤

5.1 绘制拓扑结构

根据题目当中提供的网络结构如图 10所示。

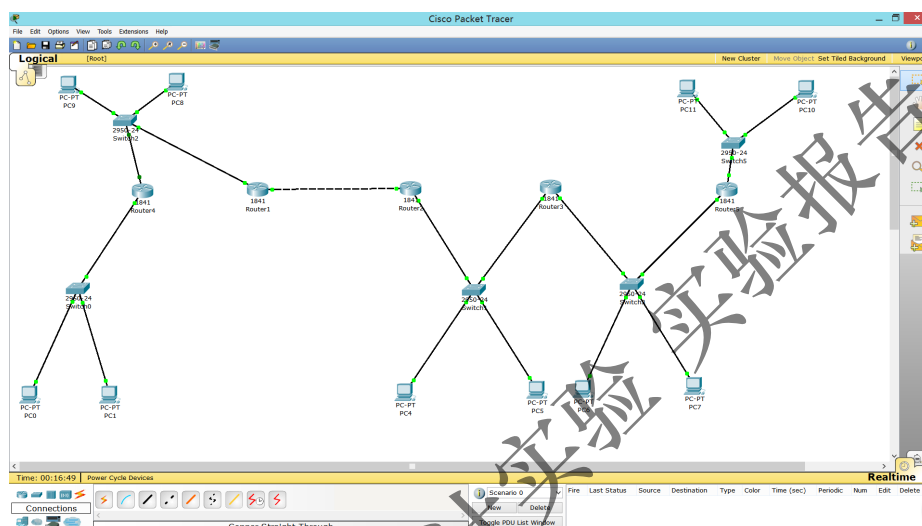


图 10: 网络拓扑结构图

5.2 搭建网络

在 Cisco Packet Tracer 5.0 软件中搭建网络结构如图 11所示。

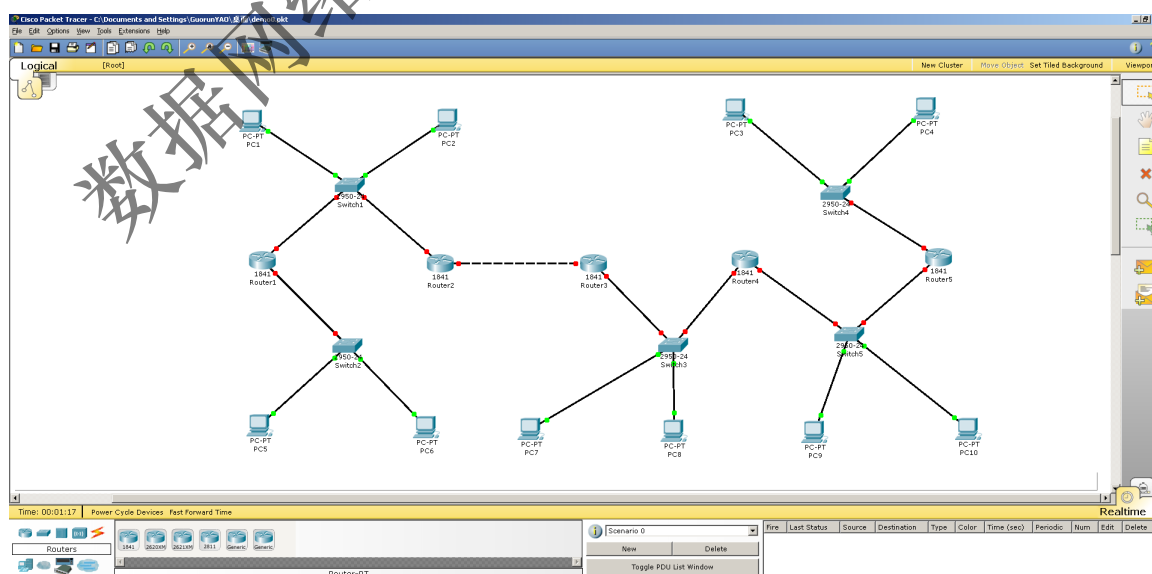


图 11: 搭建网络结构

5.3 配置 VLAN

根据实验要求，二层交换机的每个端口在不同 VLAN，所以要先对交换机进行 VLAN 的配置，配置 VID 如表格 1 所示，配置界面如图 12 所示。

表 1: VLAN 配置

名称	VLAN	
Switch1	10	20
Switch2	30	40
Switch3	50	60
Switch4	90	100
Switch5	70	80

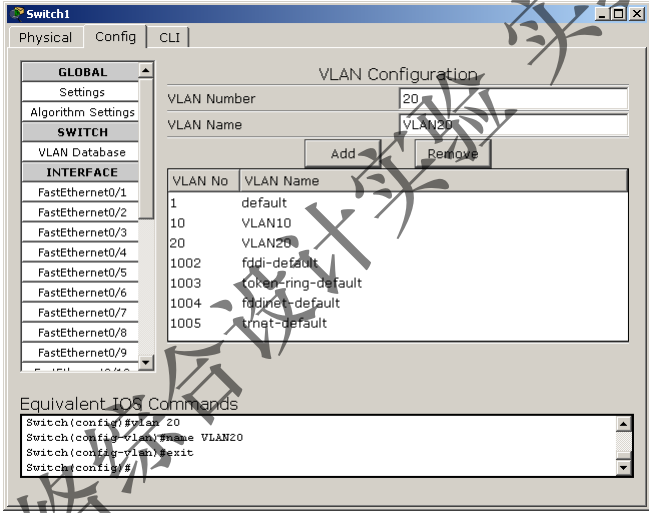


图 12: 配置 VLAN

5.4 配置交换机端口

根据上文介绍，交换机的端口有 Access 和 Trunk 两种类型，其中，与客户端相连接的端口，应当配置成 Access 型，与路由器相连接的端口，应当配置成 Trunk 型。配置界面如图所示。

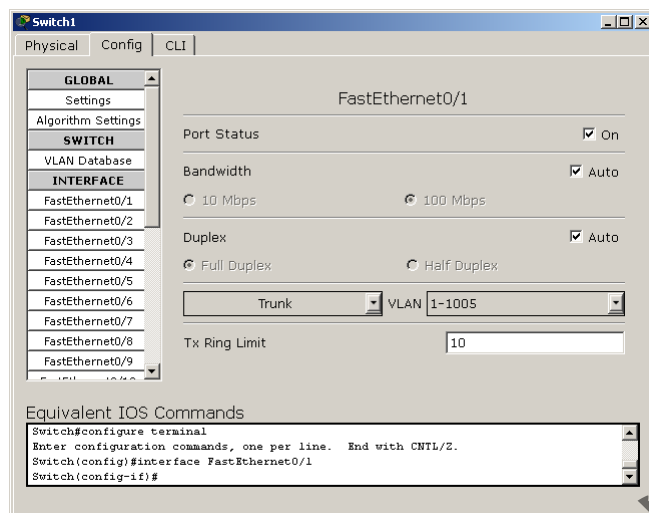


图 13: 配置交换机端口

5.5 配置路由器端口

根据实验要求，要用到单臂路由来实现互联，接下来进行子端口的配置。配置端口/子端口地址如表格 2 所示，配置命令示例如下。

```

1 //Router1 的配置
2 Router>enable
3 Router#configure terminal
4
5 Router(config)#interface fastEthernet 0/0
6 Router(config-if)#ip address 193.168.1.1 255.255.255.0
7 Router(config-if)#no shutdown
8 Router(config-if)#exit
9
10 Router(config)#interface fastEthernet 0/0.1
11 Router(config-subif)#encapsulation dot1Q 10
12 Router(config-subif)#ip address 192.168.1.254 255.255.255.0
13 Router(config-subif)#exit
14
15 Router(config)#interface fastEthernet 0/0.2
16 Router(config-subif)#encapsulation dot1Q 20
17 Router(config-subif)#ip address 192.168.2.254 255.255.255.0
18 Router(config-subif)#exit
19
20 Router(config)#interface fastEthernet 0/1
21 Router(config-if)#no shutdown
22 Router(config-if)#exit
23
24 Router(config)#interface fastEthernet 0/1.1
25 Router(config-subif)#encapsulation dot1Q 30
26 Router(config-subif)#ip address 192.168.5.254 255.255.255.0
27 Router(config-subif)#exit

```

```

28
29 Router(config)#interface fastEthernet 0/1.2
30 Router(config-subif)#encapsulation dot1Q 40
31 Router(config-subif)#ip address 192.168.6.254 255.255.255.0
32 Router(config-subif)#exit
33
34 Router(config)#exit
35
36 Router#copy running-config startup-config

```

表 2: 路由器端口配置

名称	端口	地址	VLAN	名称	端口	地址	VLAN
Router1	f0/0	193.168.1.1	-	Router4	f0/1.2	192.168.8.254	60
	f0/0.1	192.168.1.254	10		f0/0	193.168.3.2	-
	f0/0.2	192.168.2.254	20		f0/0.1	192.168.7.253	50
	f0/1.1	192.168.5.254	30		f0/0.2	192.168.8.253	60
	f0/1.2	192.168.6.254	40		f0/1	193.168.4.1	-
Router2	f0/0	193.168.1.2	-	Router5	f0/1.1	192.168.9.254	70
	f0/0.1	192.168.1.253	10		f0/1.2	192.168.10.254	80
	f0/0.2	192.168.2.253	20		f0/0	193.168.4.2	-
	f0/1	193.168.2.1	-		f0/0.1	192.168.9.253	70
Router3	f0/0	193.168.2.2	-		f0/0.2	192.168.10.253	80
	f0/1	193.168.3.1	-		f0/1.1	192.168.3.254	90
	f0/1.1	192.168.7.254	50		f0/1.2	192.168.4.254	100

5.6 配置 DHCP

表 3: DHCP 配置

名称	地址池	网络	DNS	默认路由
Router1	oned	192.168.1.0	192.168.11.253	192.168.1.254
	twod	192.168.2.0	192.168.12.253	192.168.2.254
	fived	192.168.5.0	192.168.15.253	192.168.5.254
	sixd	192.168.6.0	192.168.16.253	192.168.6.254
Router2	oned	192.168.1.0	192.168.11.253	192.168.1.254
	twod	192.168.2.0	192.168.12.253	192.168.2.254
Router3	sevend	192.168.7.0	192.168.17.253	192.168.7.254
	eightd	192.168.8.0	192.168.18.253	192.168.8.254
Router4	sevend	192.168.7.0	192.168.17.253	192.168.7.254
	eightd	192.168.8.0	192.168.18.253	192.168.8.254
	nined	192.168.9.0	192.168.19.253	192.168.9.254
	tend	192.168.10.0	192.168.20.253	192.168.10.254
Router5	threed	192.168.3.0	192.168.13.253	192.168.3.254
	fourd	192.168.4.0	192.168.14.253	192.168.4.254
	nined	192.168.9.0	192.168.19.253	192.168.9.254
	tend	192.168.10.0	192.168.20.253	192.168.10.254

根据实验要求，需要用到 DHCP 技术来分配 IP 地址，所以要按照表格 3 对每一个路由器进行 DHCP 的配置，配置命令如下。同时要设置客户端 IP 地址为 DHCP，这样才能够自动获取动态地址，设置界面如图所示。

```
1 //Router1 的配置
2 Router>enable
3 Router#configure terminal
4
5 Router(config)#ip dhcp pool aaa
6 Router(dhcp-config)#network 192.168.1.0 255.255.255.0
7 Router(dhcp-config)#dns-server 192.168.11.253
8 Router(dhcp-config)#default-router 192.168.1.254
9 Router(dhcp-config)#exit
10 Router(config)#ip dhcp excluded-address 192.168.1.254
```

```

11
12 Router(config)#ip dhcp pool bbb
13 Router(dhcp-config)#network 192.168.2.0 255.255.255.0
14 Router(dhcp-config)#dns-server 192.168.12.253
15 Router(dhcp-config)#default-router 192.168.2.254
16 Router(dhcp-config)#exit
17 Router(config)#ip dhcp excluded-address 192.168.2.254
18
19 Router(config)#ip dhcp pool eee
20 Router(dhcp-config)#network 192.168.5.0 255.255.255.0
21 Router(dhcp-config)#dns-server 192.168.15.253
22 Router(dhcp-config)#default-router 192.168.5.254
23 Router(dhcp-config)#exit
24 Router(config)#ip dhcp excluded-address 192.168.5.254
25
26 Router(config)#ip dhcp pool fff
27 Router(dhcp-config)#network 192.168.6.0 255.255.255.0
28 Router(dhcp-config)#dns-server 192.168.16.253
29 Router(dhcp-config)#default-router 192.168.6.254
30 Router(dhcp-config)#exit
31 Router(config)#ip dhcp excluded-address 192.168.6.254

```

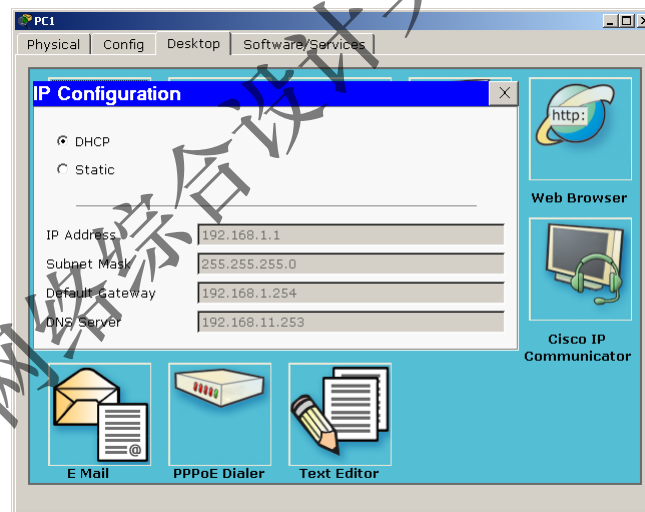


图 14: 设置 PC 为 DHCP 获取地址

5.7 配置 NAT

表 4: NAT 配置

名称	地址池	起始地址	终止地址	ACL	地址
Router1	onen	193.168.1.110	193.168.1.115	1	192.168.1.0
	twon	193.168.1.120	193.168.1.125	2	192.168.2.0
	fiven	193.168.1.150	193.168.1.155	5	192.168.5.0
	sixn	193.168.1.160	193.168.1.165	6	192.168.6.0
Router2	onen	193.168.1.110	193.168.1.115	1	192.168.1.0
	twon	193.168.1.120	193.168.1.125	2	192.168.2.0
Router3	sevens	193.168.3.170	193.168.3.175	7	192.168.7.0
	eighn	193.168.3.180	193.168.3.185	8	192.168.8.0
Router4	sevens	193.168.3.170	193.168.3.175	7	192.168.7.0
	eighn	193.168.3.180	193.168.3.185	8	192.168.8.0
	ninen	193.168.4.190	193.168.4.195	9	192.168.9.0
	tenn	193.168.4.200	193.168.4.205	10	192.168.10.0
Router5	threen	193.168.4.130	193.168.4.135	3	192.168.3.0
	fourn	193.168.4.140	193.168.4.145	4	192.168.4.0
	ninen	193.168.4.190	193.168.4.195	9	192.168.9.0
	tenn	193.168.4.200	193.168.4.205	10	192.168.10.0

根据实验要求，需要用到 NAT 技术进行地址转换，所以要按照表格 4 对每一个路由器进行 NAT 的配置，配置命令如下。其中用到了 ACL 技术，控制公网不能访问私网，私网可以访问公网。

```

1 //Router1的配置
2 Router>enable
3 Router#configure terminal
4
5 Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
6 Router(config)#ip nat pool aa 193.168.1.110 193.168.1.115 netmask 255.255.255.0
7 Router(config)#ip nat inside source list 1 pool aa
8
9 Router(config)#access-list 2 permit 192.168.2.0 0.0.0.255
10 Router(config)#ip nat pool bb 193.168.1.120 193.168.1.125 netmask 255.255.255.0
11 Router(config)#ip nat inside source list 2 pool bb
12

```

```

13 Router(config)#access-list 5 permit 192.168.5.0 0.0.0.255
14 Router(config)#ip nat pool ee 193.168.1.150 193.168.1.155 netmask 255.255.255.0
15 Router(config)#ip nat inside source list 5 pool ee
16
17 Router(config)#access-list 6 permit 192.168.6.0 0.0.0.255
18 Router(config)#ip nat pool ff 193.168.1.160 193.168.1.165 netmask 255.255.255.0
19 Router(config)#ip nat inside source list 6 pool ff

```

5.8 配置路由表

根据实验要求，需要用静态路由的方式来配置路由，所以要按照表格 5 对每一个路由器进行路由配置，配置命令如下。

```

1 //Router1 的配置
2 Router>enable
3 Router#configure terminal
4 Router(config)#ip route 192.168.3.0 255.255.255.0 193.168.1.2
5 Router(config)#ip route 192.168.4.0 255.255.255.0 193.168.1.2
6 Router(config)#ip route 192.168.7.0 255.255.255.0 193.168.1.2
7 Router(config)#ip route 192.168.8.0 255.255.255.0 193.168.1.2
8 Router(config)#ip route 192.168.9.0 255.255.255.0 193.168.1.2
9 Router(config)#ip route 192.168.10.0 255.255.255.0 193.168.1.2
10 Router(config)#ip route 193.168.2.0 255.255.255.0 193.168.1.2
11 Router(config)#ip route 193.168.3.0 255.255.255.0 193.168.1.2
12 Router(config)#ip route 193.168.4.0 255.255.255.0 193.168.1.2

```

利用命令行可以查看路由器的路由表，命令行及查询结果如下，可以清楚的看到每一个端口与其他网络相连接的途径。

```

1 Router>show ip route
2 C    192.168.1.0/24 is directly connected, FastEthernet0/0.1
3 C    192.168.2.0/24 is directly connected, FastEthernet0/0.2
4 S    192.168.3.0/24 [1/0] via 193.168.1.2
5 S    192.168.4.0/24 [1/0] via 193.168.1.2
6 C    192.168.5.0/24 is directly connected, FastEthernet0/1.1
7 C    192.168.6.0/24 is directly connected, FastEthernet0/1.2
8 S    192.168.7.0/24 [1/0] via 193.168.1.2
9 S    192.168.8.0/24 [1/0] via 193.168.1.2
10 S    192.168.9.0/24 [1/0] via 193.168.1.2
11 S    192.168.10.0/24 [1/0] via 193.168.1.2
12 C    192.168.21.0/24 is directly connected, Tunnel1
13 C    192.168.22.0/24 is directly connected, Tunnel2
14 C    192.168.23.0/24 is directly connected, Tunnel3
15 C    193.168.1.0/24 is directly connected, FastEthernet0/0
16 S    193.168.2.0/24 [1/0] via 193.168.1.2
17 S    193.168.3.0/24 [1/0] via 193.168.1.2
18 S    193.168.4.0/24 [1/0] via 193.168.1.2

```

表 5: 路由表配置

名称	目的地址	子网掩码	下一跳地址	名称	目的地址	子网掩码	下一跳地址
Router1	192.168.3.0	255.255.255.0	193.168.1.2	Router3	192.168.5.0	255.255.255.0	193.168.2.1
	192.168.4.0	255.255.255.0	193.168.1.2		192.168.6.0	255.255.255.0	193.168.2.1
	192.168.7.0	255.255.255.0	193.168.1.2		192.168.9.0	255.255.255.0	193.168.3.2
	192.168.8.0	255.255.255.0	193.168.1.2		192.168.10.0	255.255.255.0	193.168.3.2
	192.168.9.0	255.255.255.0	193.168.1.2		193.168.1.0	255.255.255.0	193.168.2.1
	192.168.10.0	255.255.255.0	193.168.1.2		193.168.4.0	255.255.255.0	193.168.3.2
	193.168.2.0	255.255.255.0	193.168.1.2		192.168.1.0	255.255.255.0	193.168.3.1
	193.168.3.0	255.255.255.0	193.168.1.2		192.168.2.0	255.255.255.0	193.168.3.1
	193.168.4.0	255.255.255.0	193.168.1.2		192.168.3.0	255.255.255.0	193.168.4.2
Router2	192.168.3.0	255.255.255.0	193.168.2.2	Router4	192.168.4.0	255.255.255.0	193.168.4.2
	192.168.4.0	255.255.255.0	193.168.2.2		192.168.5.0	255.255.255.0	193.168.3.1
	192.168.5.0	255.255.255.0	193.168.1.1		192.168.6.0	255.255.255.0	193.168.3.1
	192.168.6.0	255.255.255.0	193.168.1.1		193.168.1.0	255.255.255.0	193.168.3.1
	192.168.7.0	255.255.255.0	193.168.2.2		193.168.2.0	255.255.255.0	193.168.3.1
	192.168.8.0	255.255.255.0	193.168.2.2	Router5	192.168.1.0	255.255.255.0	193.168.4.1
	192.168.9.0	255.255.255.0	193.168.2.2		192.168.2.0	255.255.255.0	193.168.4.1
	192.168.10.0	255.255.255.0	193.168.2.2		192.168.5.0	255.255.255.0	193.168.4.1
	193.168.3.0	255.255.255.0	193.168.2.2		192.168.6.0	255.255.255.0	193.168.4.1
	193.168.4.0	255.255.255.0	193.168.2.2		192.168.7.0	255.255.255.0	193.168.4.1
Router3	192.168.1.0	255.255.255.0	193.168.2.1		192.168.8.0	255.255.255.0	193.168.4.1
	192.168.2.0	255.255.255.0	193.168.2.1		193.168.1.0	255.255.255.0	193.168.4.1
	192.168.3.0	255.255.255.0	193.168.3.2		193.168.2.0	255.255.255.0	193.168.4.1
	192.168.4.0	255.255.255.0	193.168.3.2		193.168.3.0	255.255.255.0	193.168.4.1

5.9 配置 GRE 隧道

表 6: GRE 隧道配置

名称	隧道编号	源地址	目的地址
Router1	1	f0/0	193.168.2.2
	2	f0/0	193.168.3.2
	3	f0/0	193.168.4.2
Router2	4	f0/1	193.168.3.2
	5	f0/1	193.168.4.2
Router3	6	f0/0	193.168.1.1
	7	f0/1	193.168.4.2
Router4	8	f0/0	193.168.1.1
	9	f0/0	193.168.2.1
Router5	10	f0/0	193.168.1.1
	11	f0/0	193.168.2.1
	12	f0/0	193.168.3.1

根据实验要求，需要用到 GRE 隧道技术，所以要按照表格 6 对每一个路由器建立 GRE 隧道，配置命令如下。

```
1 //Router1 的配置
2 Router>enable
3 Router#configure terminal
4
5 Router(config)#interface tunnel 1
6 Router(config-if)#ip address 192.168.21.1 255.255.255.0
7 Router(config-if)#tunnel source fastEthernet 0/0
8 Router(config-if)#tunnel destination 193.168.2.2
9 Router(config-if)#no shutdown
10 Router(config-if)#exit
11
12 Router(config)#interface tunnel 2
13 Router(config-if)#ip address 192.168.22.1 255.255.255.0
14 Router(config-if)#tunnel source fastEthernet 0/0
15 Router(config-if)#tunnel destination 193.168.3.2
16 Router(config-if)#no shutdown
17 Router(config-if)#exit
18
19 Router(config)#interface tunnel 3
```

```

20 Router(config-if)#ip address 192.168.23.1 255.255.255.0
21 Router(config-if)#tunnel source fastEthernet 0/0
22 Router(config-if)#tunnel destination 193.168.4.2
23 Router(config-if)#no shutdown
24 Router(config-if)#exit

```

可以通过命令查看路由器的接口情况，其中包含隧道及其状态，命令及查询结果如下。

```

1 Router>enable
2 Router#show ip interface brief
3
4 Interface                IP-Address      OK? Method Status  Protocol
5
6 FastEthernet0/0          193.168.1.1     YES manual up      up
7
8 FastEthernet0/0.1        192.168.1.254   YES manual up      up
9
10 FastEthernet0/0.2        192.168.2.254   YES manual up      up
11
12 FastEthernet0/1          unassigned      YES unset  up      up
13
14 FastEthernet0/1.1        192.168.5.254   YES manual up      up
15
16 FastEthernet0/1.2        192.168.6.254   YES manual up      up
17
18 Tunnel1                  192.168.21.1     YES manual up      up
19
20 Tunnel2                  192.168.22.1     YES manual up      up
21
22 Tunnel3                  192.168.23.1     YES manual up      up
23
24 Vlan1                    unassigned      YES unset  administratively down down

```

5.10 测试网络

逐个测试 PC 之间、路由器之间以及 PC 与路由器的通信情况，发现通信正常，任意两个节点之间能够在规则下互相访问。

6 心得体会

本次实验搭建了一个比较复杂的网络。

在网络中用到了 VLAN 技术，用于划分广播域，同时，交换机在这里起到了拓展路由器接口的作用，可以将路由器的子接口进行进一步的划分，并且保证信息互不干扰。路由器直接相连，则无需设置子端口，如果路由器和交换机相连，交换机又连接了多台计算机，这些计算机分别处于交换机所分配的不同 VLAN 中，这时候需要设置路由器的子端口。路由器的路由表中，我们主要设置下一跳地址和目标网络两个，由于交换机并不能连接不同网络，所以可知，路由器的下一跳地址可以设置为与其连接在同一交换机的另一台路由器的一个端口地址，这里可以看成两台路由器间接连接。

在实验中遇到了一个问题，就是两台路由器的子端口地址，不能分配为同一地址，因为地址是独一无二的，起到标识作用，这里出现了一个问题，将和同一台交换机相连的两台路由器的端口地址设为相同地址，这样导致在创建路由表时出现下一跳地址与本端口地址相同的情况，应当引起注意。

数据网络综合设计实验 实验报告