



计算机通信与网络课程设计

- 一个中小型企业网络规划与设计的方案

专 业： 计算机科学与技术

班 级： 计科 1801

学 号： 181303130

姓 名： 周洲

同组成员： 曹颖 刘絮 龙瑶 赵雯飞 陆欣雨

指导教师： 杨云教授

完成日期： 2021 年 1 月 6 日

序号	项目名称	考核比重	得分
1	方案设计	30%	29
2	网络搭建	30%	28
3	设计验收	20%	19
4	设计报告	20%	19
	总成绩	100%	95

《计算机通信与网络》课程设计题目

序号	课程设计题目
题目一	一个中小型企业网络规划与设计的方案

1、课程设计任务

某公司有 800 台 PC；公司共有 8 个部门，不同部门的相互访问要求有限制，公司有 2 个跨省的分公司；公司有自己的内部网页与外部网站，公司能够提供匿名的 FTP、E-mail、WWW 服务，但 FTP 只对内部员工开放；公司有自己的 OA 系统；公司中的每台主机都能登录 Internet，每个部门的办公室联合构成一个 VLAN；核心技术采用 VPN。

2、软硬件环境及开发工具

- (1) 仿真软件：Cisco packet tracer；
- (2) 开发环境：TCP/IP 协议、Windows 7 及以上；

3、要求：

(1) 在 Cisco Packet Tracer 路由模拟器软件上，按照课程设计任务要求，构建完成公司的 LAN；

(2) 课程设计报告中必须包括的内容：

① 网络配置：综合布线、IP 地址规划及子网划分、硬件设计；（截图说明）

部门名称	主机数(台)	IP 地址范围	子网掩码	VLAN
总公司部门 1				
总公司部门 2				
.....				
分公司 1				
.....				

② 网络拓扑：层次模型、拓扑结构、物理设备、物理介质和功能区域划分（截图说明）

层次模型：一般为核心层、汇聚层和接入层；

拓扑结构：一般为总线型、星型、环型、网状型；

物理设备：一般有交换机、路由器、服务器、防火墙、网关、网桥、网闸等；

物理介质：一般有双绞线、同轴电缆、光纤；

③ 物理设备选型

设备名称	型号	主要技术参数	数量	价格
PC 机				
服务器				
交换机				
路由器				
双绞线				
光纤				
.....				

④ 交换机配置信息

交换机名称	型号	E0/0/0	E0/0/1	F1/0/0	F1/0/1
Ethernet1						
Ethernet2						
.....						

⑤ 路由器配置信息

路由器名称	型号	E0/0/0	E0/0/1	F1/0/0	F1/0/1
Router1						
Router2						
....						

⑥ 服务器配置信息

Pool Name	Server Pool
DNS 服务器	
Web 服务器	
FTP 服务器	
SMTP 服务器	
.....	
默认网关	
子网掩码	

⑦ 防火墙等配置信息（可选项）

⑧ 系统测试：网络连通性测试（LAN、VLAN）、邮件服务测试、Web 服务测试、NAT 测试、FTP 服务测试；（截图说明）

⑨ 设计中的问题及其解决方案

《计算机通信与网络课程设计》答辩记录表

专业	计算机科学与技术	学号	181303130
姓名	周洲	班级	计科 1801
组号	1	题目	一个中小型企业网络规划 与设计的方案

答辩记录:

问题 1: LAN 的网络拓扑主要有哪几种? 有什么特点?

答: 常见的局域网拓扑结构有总线型、星形、环形。

①总线型结构: 总线型结构由一条高速公用主干电缆即总线连接若干个结点构成网络。网络中所有的结点通过总线进行信息的传输。这种结构的特点是结构简单灵活, 建网容易, 使用方便, 性能好。其缺点是主干总线对网络起决定性作用, 总线故障将影响整个网络。总线型结构是使用最普遍的一种网络。

②星型结构: 星型结构由中央结点集线器与各个结点连接组成, 这种网络各结点必须通过中央结点才能实现通信。星型结构的特点是结构简单、建网容易, 便于控制和管理。其缺点是中央结点负担较重, 容易形成系统的“瓶颈”, 线路的利用率也不高。

③环形结构: 环型拓扑由各结点首尾相连形成一个闭合环型线路。环型网络中的信息传送是单向的。这种结构的特点是结构简单, 建网容易, 便于管理。其缺点是当结点过多时, 将影响传输效率, 不利于扩充。树型拓扑, 树型拓扑是一种分级结构。在树型结构的网络中, 任意两个结点之间不产生回路, 每条通路都支持双向传输。这种结构的特点是扩充方便、灵活, 成本低, 易推广, 适合于分主次或分等级的层次型管理系统; 网型拓扑, 主要用于广域网, 由于结点之间有多条线路相连, 所以网络的可靠性较高。由于结构比较复杂, 建设成本较高。

问题 2: 一般地进行网络应用模型设计时, 需要考虑核心层、汇聚层和接入层的设计, 请说明这三层的主要功能:

答: 核心层是网络主干部分, 是整个网络性能的保障。核心层的主要功能在于通过高速转发通信, 提供快速、可靠的骨干传输结构, 因此核心层具有可靠性、高效性、冗余性、容错性、可管理性、适应性、低延时性等。

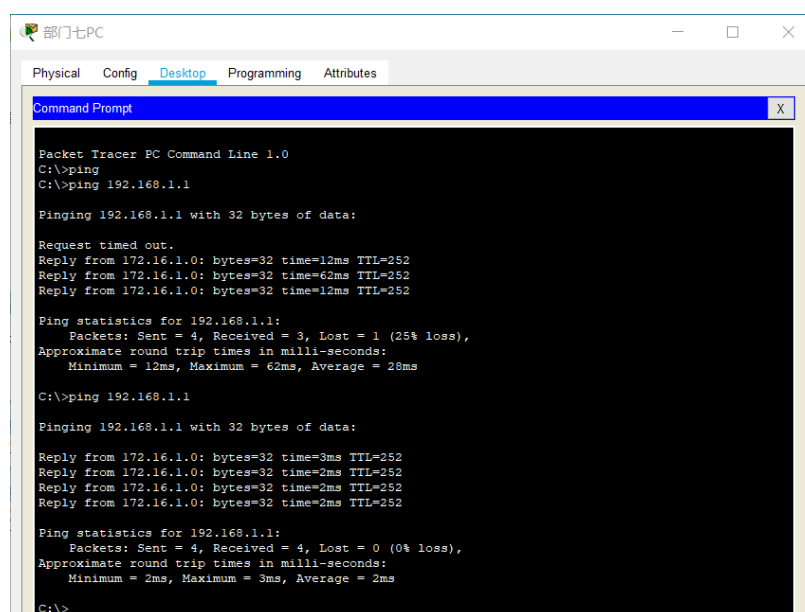
汇聚层用来连接核心层和接入层，处于中间位置，它的上行是核心交换机，下行是接入层交换。汇聚层具有实施策略、安全、工作组接入、虚拟局域网之间的路由、源地址或目的地址过滤等多种功能，它是实现策略的地方。

接入层直接面向用户连接或访问网络，接入层为用户提供了在本地网段访问应用系统的能力，主要解决相邻用户之间的互访需求，并且为这些访问提供足够的带宽。

问题 3：说明系统测试中的“网络连通性测试（LAN、VLAN）、邮件服务测试”过程，要求附运行结果截图；

答：（1）连通性测试（LAN）

①部门七 PC 位于分公司，部门一 PC 位于总公司，ip 地址分别为 192.168.1.1，192.168.7.2，下图是分公司 PC ping 总公司 PC，第一次的时候丢包一个，第二次的时候没有丢包，全部收到，ping 通。



```
Packet Tracer PC Command Line 1.0
C:\>ping
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 172.16.1.0: bytes=32 time=12ms TTL=252
Reply from 172.16.1.0: bytes=32 time=62ms TTL=252
Reply from 172.16.1.0: bytes=32 time=12ms TTL=252

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 62ms, Average = 28ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

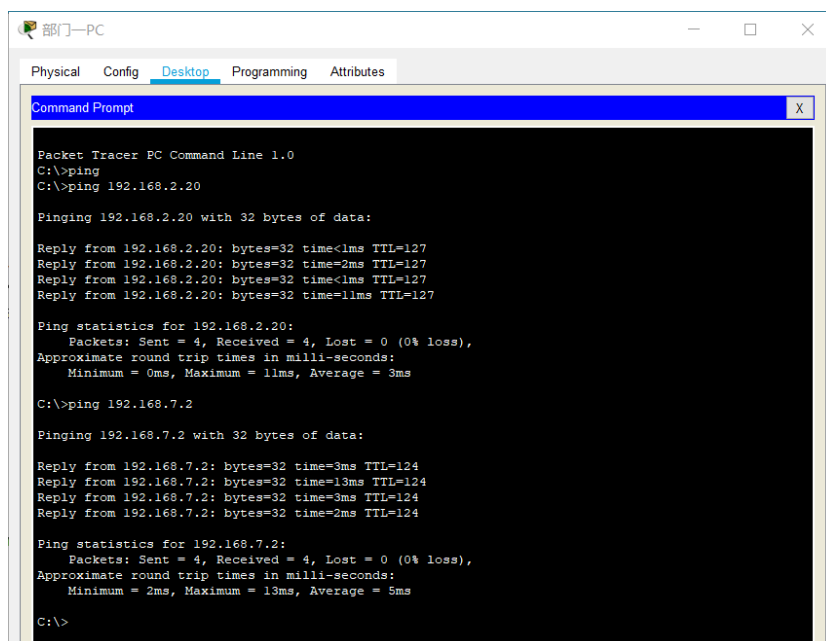
Reply from 172.16.1.0: bytes=32 time=3ms TTL=252
Reply from 172.16.1.0: bytes=32 time=2ms TTL=252
Reply from 172.16.1.0: bytes=32 time=2ms TTL=252
Reply from 172.16.1.0: bytes=32 time=2ms TTL=252

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

图 1 部门七 ping 部门一

②部门七 PC 位于分公司，部门一 PC 位于总公司，ip 地址分别为 192.168.1.1，192.168.7.2，下图是总公司 PC ping 分公司 PC,没有丢包，全部收到，ping 通。



```
Packet Tracer PC Command Line 1.0
C:\>ping
C:\>ping 192.168.2.20

Pinging 192.168.2.20 with 32 bytes of data:

Reply from 192.168.2.20: bytes=32 time<1ms TTL=127
Reply from 192.168.2.20: bytes=32 time=2ms TTL=127
Reply from 192.168.2.20: bytes=32 time<1ms TTL=127
Reply from 192.168.2.20: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.2.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>ping 192.168.7.2

Pinging 192.168.7.2 with 32 bytes of data:

Reply from 192.168.7.2: bytes=32 time=3ms TTL=124
Reply from 192.168.7.2: bytes=32 time=13ms TTL=124
Reply from 192.168.7.2: bytes=32 time=3ms TTL=124
Reply from 192.168.7.2: bytes=32 time=2ms TTL=124

Ping statistics for 192.168.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 5ms

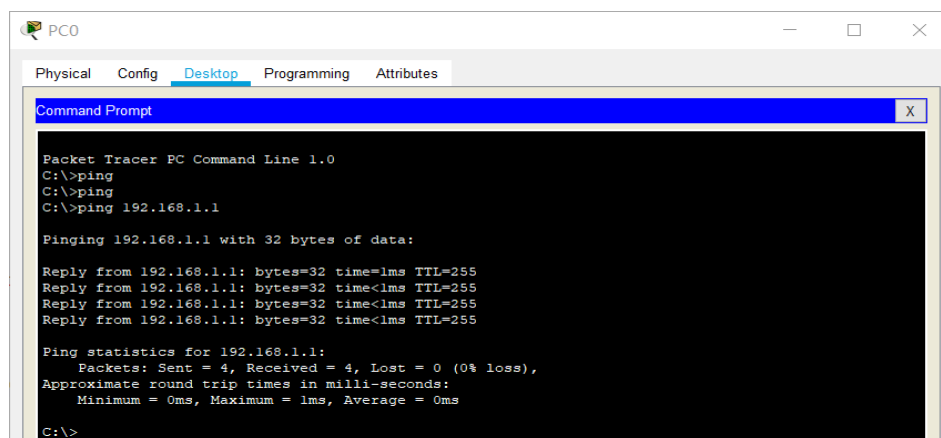
C:\>
```

图 2 部门一 PC ping 分公司 PC

(2) 连通性测试 (VLAN)

① 同一 VLAN 之间 PC 连通性测试

PC0 和 PC1 位于同一个 VLAN 内，一个 ip 地址为 192.168.1.1，一个 ip 地址为 192.168.1.20，进行 ping，发现所有包都成功收到，ping 通。



```
Packet Tracer PC Command Line 1.0
C:\>ping
C:\>ping
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

图 3 PC0 ping PC1

② 不同 VLAN 之间 PC 连通性测试

PC 和部门二 PC 位于不同 VLAN 内，一个 ip 地址为 192.168.1.20，一个 ip

地址为 192.168.2.20，进行 ping，发现所有包都成功收到，ping 通。

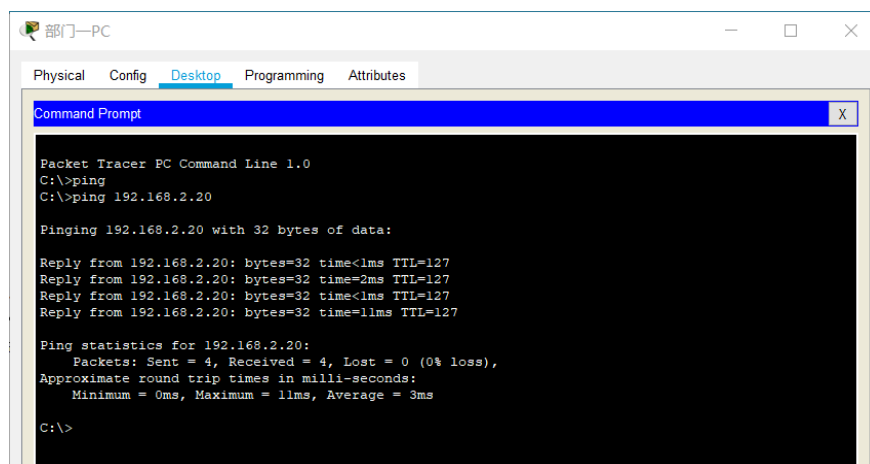


图 4 部门一 ping 部门二

(3) mail 服务测试

在部门一的 PC 上登录 mail 的账户。

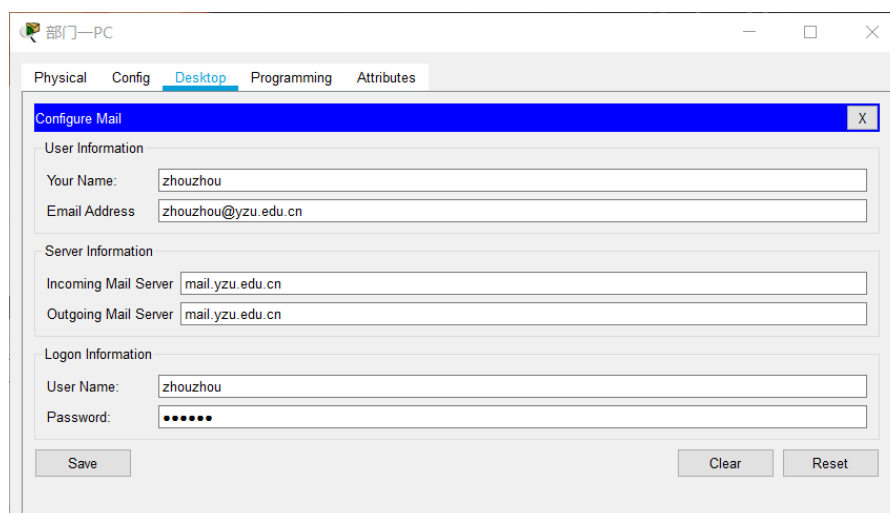


图 5 填写 mail 的账户信息

写收信人地址和主要内容，这里向 lxy 发送了一封主题为 hello world 的邮件。

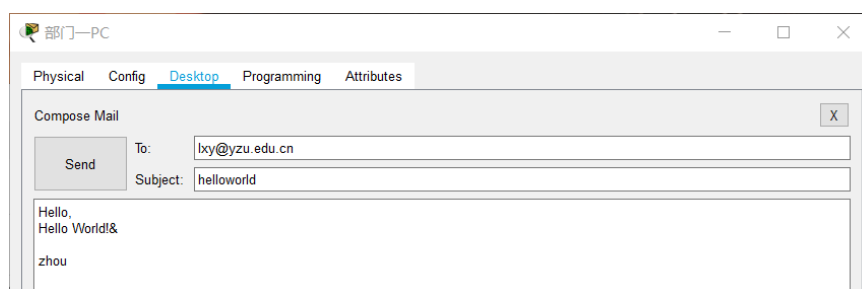


图 6 使用 mail 进行发送邮件

发送完成后，在该截图下方显示发送成功(最左下角)

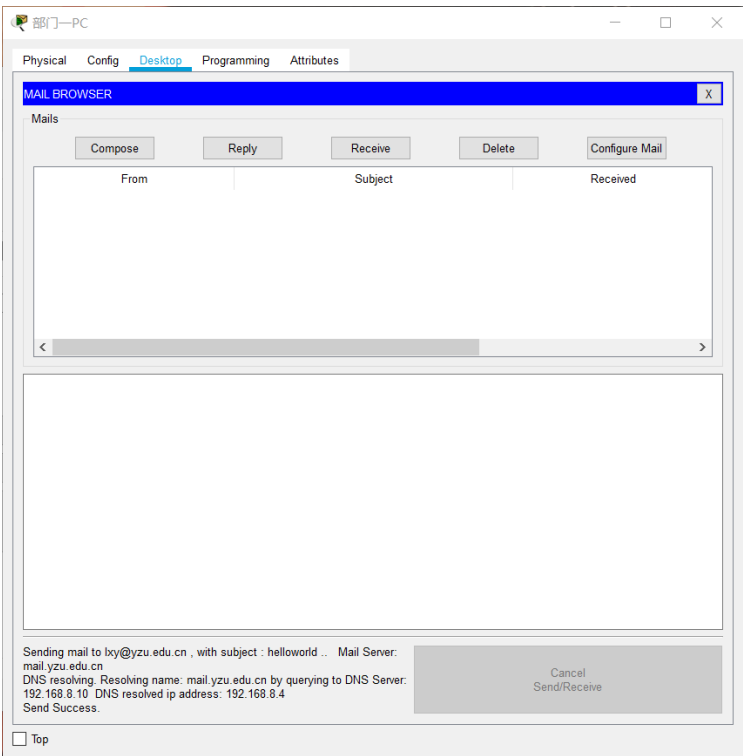


图 7 mail 发送邮件成功

可以看到 00:41:30 时刻从<zhouzhou@yzu.edu.cn>发来一封内容为“HELLOWORLD”的邮件

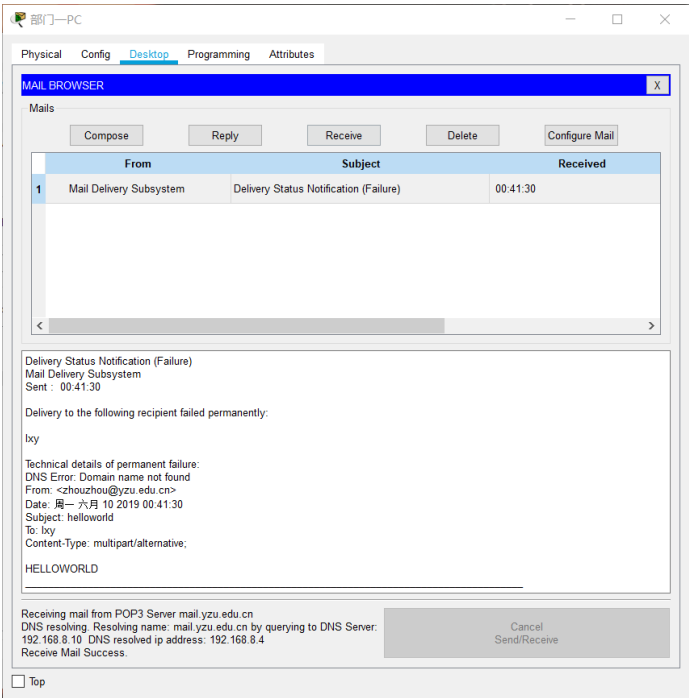


图 8 mail 接收邮件

问题 4：实验中碰到了什么问题？如何解决的？

答：起初我们不了解端口的 access 和 trunk 模式，通过互联网教学视频、书本、思科教程等渠道进行了学习和研究，终于了解了两个模式的区别。

(1) access 端口：

通过 access 端口的数据包都是不带 VLAN tag 的，且只属于一个 VLAN；

在 access 端口进方向，交换机接收到数据包后，先判断是否带 VLAN tag，有则丢弃数据包，没有则打上该端口已配置的 VLAN tag；

在 access 端口出方向，交换机将打了与端口相同 VLAN tag 的数据包转发出去，并且去掉 VLAN tag 变成普通数据包。

(2) trunk 端口：

通过 trunk 端口的数据包都必须带上 VLAN tag；

在 trunk 端口进方向，交换机接收到数据包后，先判断是否带 VLAN tag，没有则丢弃数据包，有则按照对应 VLAN 进行转发；

在 trunk 端口出方向，交换机将带 VLAN tag 的数据包原封不动转发出去，没有带 VLAN tag 数据包不会从 trunk 端口转发出去。

在 trunk 端口上有一种特殊情况，如果配置了 native VLAN（也叫 PVID），转发方式等同于 access 端口，当从端口进来的报文不带 vlan tag 时，就打上 Native vlan tag；当从端口出去的报文带 Native vlan tag 时，会剥离 TAG。

在设置路由器的各个端口的时候也出现了问题，老是会出现 overlap 这个词，查阅了资料之后知道原因。因为路由器是用来连接不同网络的，所以同一路由器的不同接口不能配置为相同的网段。改变一下网络号，就可以了。

答辩人：

日期：2021-1-6

目录

第 1 章	前言	1
1.1	背景分析	1
1.2	采用的方法和原则	1
1.3	小组分工	3
第 2 章	用户需求分析	4
2.1	功能性需求	4
2.2	非功能性需求	5
2.2.1	拓扑结构需求	5
2.2.2	综合布线需求	6
第 3 章	网络拓扑结构设计	7
3.1	拓扑结构	7
3.1.1	服务器局部图	8
3.1.2	总公司部门局部图	8
3.1.3	分公司部门局部图	9
3.1.4	外网局部图	9
3.2	硬件结构	10
3.3	地址规划	14
3.4	网络设备配置	15
第 4 章	网络物理设计	26
4.1	传输介质选择	26
4.2	综合布线设计	27
4.2.1	总公司布线设计	27
4.2.2	分公司布线设计	28
第 5 章	系统测试	29
5.1	测试工具	29
5.1.1	ping 指令	29

5.1.2 cisco 模拟桌面	29
5.2 有关服务器的连通性测试	30
5.2.1 外部服务器访问 PC 机的测试	30
5.2.2 内部服务器访问 PC 机的测试	31
5.2.3 外部服务器和内部服务器之间的连通性测试.....	32
5.3 PCi 与其它 PC 机的连通性测试.....	34
5.3.1 同一个 VLAN 之间 PC 连通性测试.....	34
5.3.2 不同 VLAN 之间 PC 连通性测试.....	35
5.3.3 分公司 PC 和总公司 PC 之间的连通性测试.....	35
5.3.4 有关 VPN 的连通性测试.....	36
5.4 功能测试	38
5.4.1 web browser 测试	38
5.4.2 访问 OA 系统进行交互.....	39
5.4.3 FTP 服务测试	40
5.4.4 mail 服务测试	41
5.4.5 DHCP 的测试	43
5.4.6 NAT 测试.....	44
5.5 测试及分析中的注意事项	45
第 6 章 网络其他设计.....	46
6.1 安全性设计	46
6.2 可靠性设计	47
第 7 章 总结与体会.....	49
参考文献.....	51

第1章 前言

本章对于本课程设计的背景，采用的方法和原则以及小组分工进行了概述，阐述了课程设计的目的和意义。

1.1 背景分析

随着信息时代的到来，网络已经成为现代企业背景下的必要基础设施，成为企业提高自身发展水平的重要途径。企业网络的主干所承担的信息流量很大，企业网络的建设的目标是实现办公的自动化、无纸化。能通过 Internet 的互联，为企业职工提供国际互联网上的各种服务。企业领导可以通过网络这个平台给职工下达命令，实现企业资源共享。企业网络组建能为企业的信息化建设打下坚实的基础^[1]。

1.2 采用的方法和原则

本课设以网络的实用性、扩展性、可靠性、安全性为基本原则，合理利用现有的资源和环境，在保障各部门正常工作的前提下，对现有网络架构的基础上进行改进和拓展，极大的降低了设计失败而产生的风险和损失。由于计算机网络的特殊性，网络建设需要考虑以下因素：系统的先进性、系统的稳定性、系统的可扩展性、系统的可维护性、应用系统和网络系统的适配度、与外界网络的连通性以及建设的成本等问题^[2]。

1、选择高带宽网络设计

企业网应用具体要求决定了网络必须采取高带宽网络。在构建企业网时，不能犹豫网络传输速率不足，而影响整个网络的整体性能。所以要尽可能的采用最新的高带宽网络技术。

2、选择可扩充的网络架构

企业网的用户数量或者服务功能是逐渐提高的，网络技术日新月异，新技术新产品不断涌现。一般情况下，企业网的建设资金用量非常大，所以这就要求在

网络架构上选择具有良好的可扩展性的网络互联设备，有效的利用现有的投资，并可持续发展。

3、充分共享网络资源

组建计算机网络的主要目的就是实现资源共享。资源共享包括硬件资源、软件资源。网络用户通过网络不仅可以实现文件共享。数据共享，还可以通过网络实现设备的共享，如打印机、扫描仪等。

4、网络可管理性

降低网络运营成本和维护成本是网络设计中必须考虑的一个环节。只要在网络设计时选用支持网络管理功能的网络设备，才能将来降低网络运行即维护成本打下坚实的基础^[3]。

5、网络系统和应用系统的整合

企业网构建了企业内部数据的通路，为应用系统发挥更大的作用打下了基础。网络系统和应用系统要能够很好的融合，才能发挥企业网的效率和优势。

6、建设成本

考虑企业网工程在建设方面都希望成本比较低，整个网络系统有较高的性价比，所以在设备选型等方面选用性价比较高的网络产品。

7、高可靠性

网络要求高可靠性、高稳定性和足够的设备冗余和备份，防止因局部故障引起整个网络系统的瘫痪，避免网络上出现单点失效的情况。所以在网络干线上要提供适当的冗余配置。采用各种有效的安全措施，保证网络系统和应用系统安全运行。

1.3 小组分工

成员	分工
周洲	网络模型搭建
龙瑶	总体设计
曹颖	测试
刘絮	需求分析
赵雯飞	设备选型
陆欣雨	网络模型搭建

第2章 用户需求分析

课程设计中用户需求分析是最重要的，只有搞清楚用户的需求，才能根据用户的需求，进行系统的功能划分、概要设计、详细设计等。本章主要分为两个部分，一个是功能性需求，一个是非功能性需求，通过图文结合等部分形象说明当前课程设计的需求。

2.1 功能性需求

- ①公司共有 8 个部门，不同部门的相互访问要求有限制；
- ②公司有自己的内部网页与外部网站，能够提供匿名的 FTP、E-mail、WWW 服务，但 FTP 只对内部员工开放，采用 OA 系统；
- ③公司中的每台主机都能登录 Internet，每个部门的办公室联合构成一个 VLAN；
- ④核心技术采用 VPN。

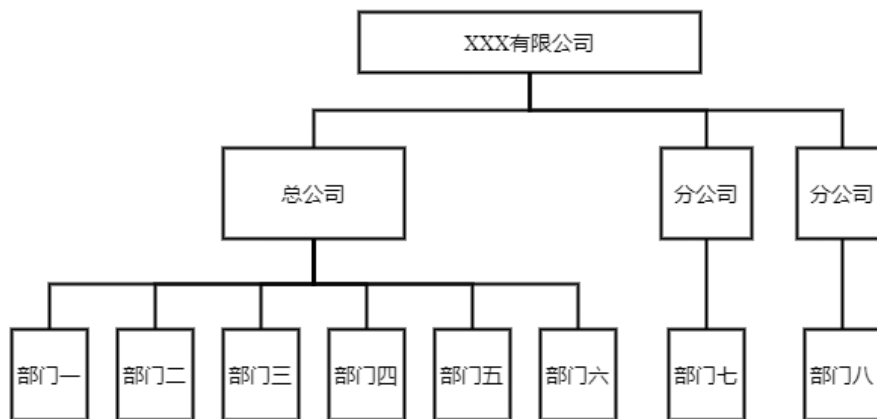


图 2.1 公司架构图

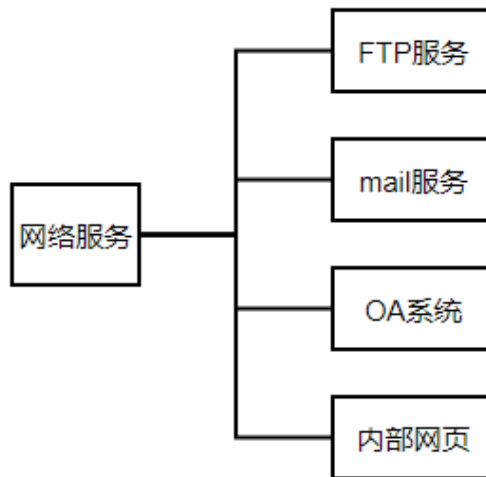


图 2.2 公司网站功能模块图

2.2 非功能性需求

可靠性：要求网络在发生一定的故障时，仍然能够保证承载的业务不中断。

可扩展性：要求网络能够支持不断增加的业务量。

可运营性：保证网络的运行和维护。

可管理性：要求网络提供标准的管理手段，便于监控和维护。

安全性：要求网络分别针对不同的应用和不同的网络通信环境，采取不同的措施，能够对重要信息进行保护。

2.2.1 拓扑结构需求

为了方便总公司对分公司和下属部门的管理，在网络拓扑结构上采用星型网络拓扑结构。星型网络拓扑结构具有安全、可靠、易扩展等特点，以交换机为中心，服务器和 PC 工作站直接连接至交换机，组成网络。通过相应的配置，在不改变网络节点物理位置的情况下，可对网络的逻辑结构进行合理的划分，即建立虚拟网络，以达到网络信息流量的有效控制^[6]。如下图所示一个星形拓扑网络结构示意图，在本次实践中，使用了更大规模，更加复杂的星型拓扑。

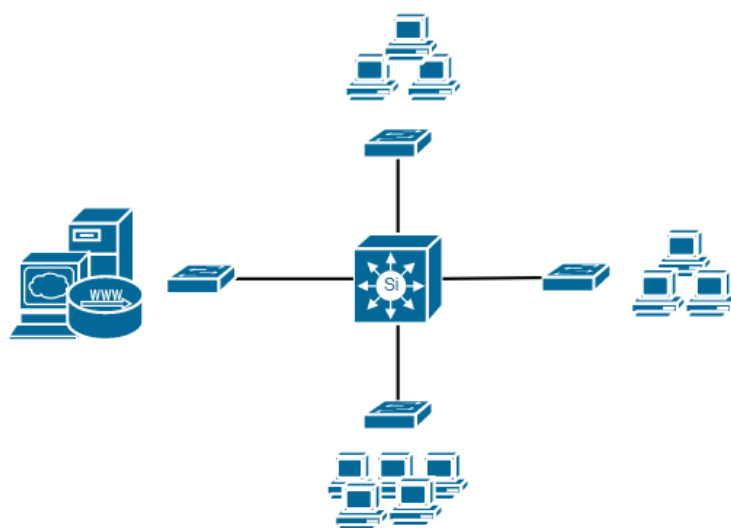


图 2.3 星型拓扑结构

2.2.2 综合布线需求

在该网络拓扑的设计下，需要使用两种不同的网线连接，对于网线来说，目前由于终端设备驱动都能智能识别线序，直通线可以连接任何两个现代的网络设备，所以我们大部分使用直通线连接，值得一提的是，目前直通线的最大传输速率均普遍超过 10Gbps，即使面对百台设备的满负荷运转，每台设备依然可以分到大于 20 兆的带宽，足以满足普通的网络带宽需求。只有使用串行口连接路由器时，才使用 V.35 的电缆。

第3章 网络拓扑结构设计

由于不同的网络拓扑其性能是不一样的，所以选择合适的网络拓扑，直接影响到网络的功能、网络的实现。而网络系统的硬件选择影响到网络实现成本、网络的性能。本章分为拓扑结构和硬件结构两部分，采用课程设计中实例分析使用到的星形拓扑结构，硬件的配置是本次课程设计的重点，详细分析了配置的代码，说明配置方法的原因和目的，使用表格图片形式说明具体配置。

3.1 拓扑结构

本课设共设计了八个部门，一个网络中心，一个服务器集群^[13]。整体的拓扑结构为星形结构。在每个部门中，都是以部门交换机为中心发散。在整体布局中，以三层交换机为核心进行发散。下图中，右上角绿色的是总公司的服务器集群，左上角的绿色的是外网，左下角的是两个分公司，右下角的棕色的是总公司。

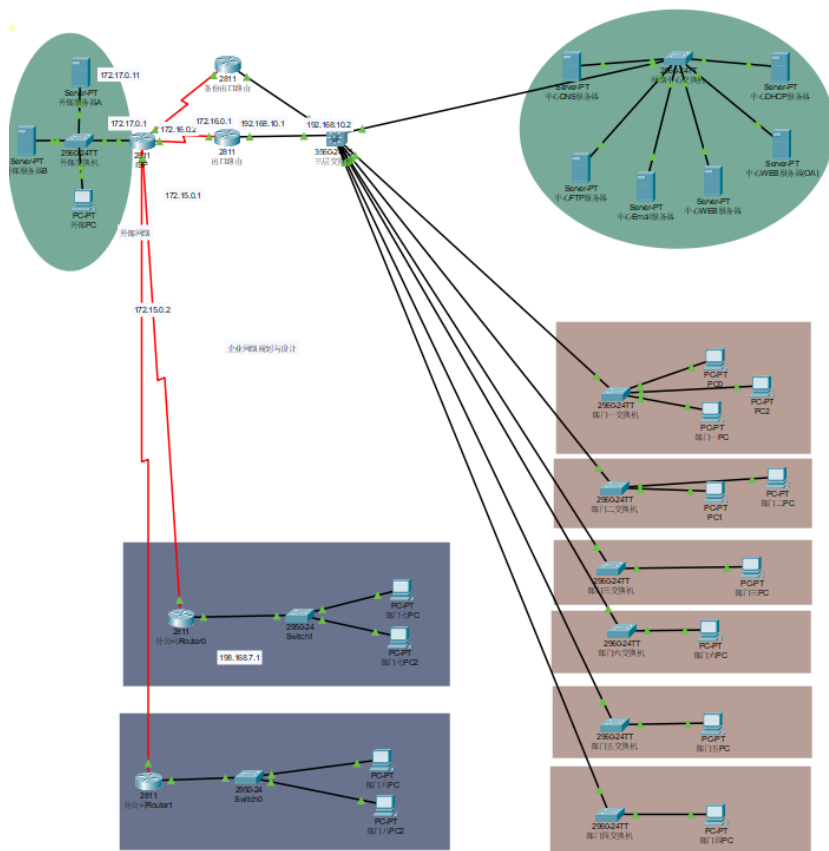


图 3.1 整体拓扑图

3.1.1 服务器局部图

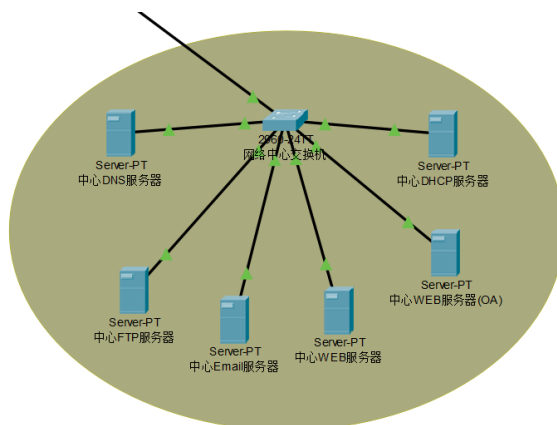


图 3.2 服务器集群局部图

如上图所示，服务器集群共有六个服务器，分别是 DNS 服务器（负责域名解析），Email 服务器（负责公司内部邮件收发），web 服务器（负责公司网页），web(OA)服务器（OA 系统专门的服务器），DHCP 服务器（给各个 VLAN 动态分配地址），FTP 服务器（负责 FTP 服务）。

3.1.2 总公司部门局部图

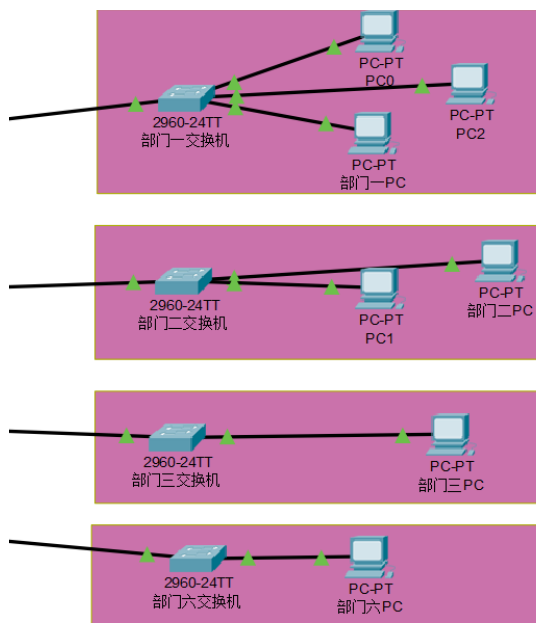


图 3.3 总公司部门局部图

在我们的设计中，总公司共分为 6 个部门，每个部门都有一个 2960-24TT

交换机，每台交换机最多能够为 256 台 PC，或者是笔记本提供服务，在本次实验中，每个部门只放置了个位数的 PC 机作为示意，事实上，由于采用了 DHCP 服务器为设备动态分配 IP 分地址，当需要扩充 PC 数量时，只需要直接添加 PC 机，连到所在部门的交换机上，等待 DHCP 分配的 IP 地址即可，无需进行额外的配置。

3.1.3 分公司部门局部图

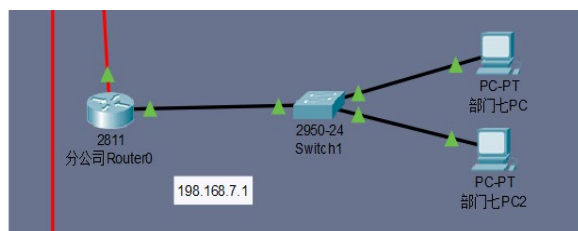


图 3.4 分公司部门局部图

如上图所示，是我们设计的一个分公司的局部图，每个分公司都有一台独立路由器，在这台路由器上设置了 VPN，可以连接到总公司，使其忽略物理距离上的差别，可以畅通的使用总公司的 OA，FTP，mail 服务，也可以和总公司的 PC 机进行通信。对于分公司，同样也只画了个位数的 PC 机，但理论上这台 2960-24TT 交换机能够给 256 台 PC 机提供服务，扩展同样可行且相当容易。

3.1.4 外网局部图

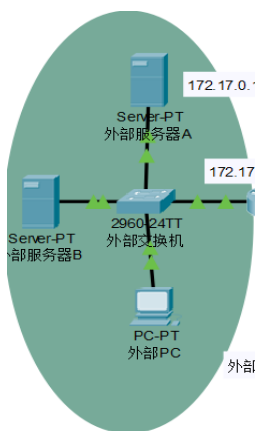


图 3.5 外网局部图

我们设计了如图所示的结构作为外网的一个简单表示,该结构拥有两台外部服务器与一台外部 PC,在实际生活中的 Internet,是由有无数台路由器,无数台路由器构成的,经过路由到达这里。这里放置两台路由器和一台外部 PC 仅作为示意,在后面的章节中会详细叙述有关 NAT 配置,路由表的配置内容。

3.2 硬件结构

表 3.1 硬件设备信息表

设备名称	型号	主要技术参数	数量	价格(元)
服务器	Server-PT	产品类型:机架式,产品结构:40,CPU 型号 Xeon E7-4809 v2,CPU 频率 1.9GHz,CPU 核心六核,内存容量为 4GB,硬盘容量 600 关闭,显示芯片期 Matrox G200, 8MB 显存,电源功率 1100W	8	14000/台
路由器	2811	路由器类型:多业务路由器,端口结构:模块化,局域网接口:2 个,其它端口:2 个固定 USB1.1 端口,扩展模块:2 个板载 AIM(内部)插槽+4 个接口卡插槽+1 个插槽(支持 NM 和 NME 模块),产品内存: DRAM: 最大 760MB, 缺省 256MB, 闪存: 最大 128MB, 缺省 64MB, 电源电压: AC 100-240V, 47-63Hz, 电源功率: 160W	5	7280/台
交换机	3560-24ps	DRAM 内存: 128MB, 接口类型: 10/100BASE-TX 端口,10/100Base-T 端口,接口数目: 24 口,传输速率: 10M/100M/1000Mbps,扩展插槽: 2,堆叠支持: 不可堆叠	1	1750/台
交换机	2960-24TT	传输速率: 10Mbps/100Mbps/1000Mbps,交换机类型: 智能交换机.内存: 64M, 端口数量: 24, 接口介质: 10/100Base-T、10/100/1000Base-Tx, 传输模式: 全双工/半双工自适应, 交换方式: 存储-转发, 背板带宽: 16Gbps	8	1750/台
交换机	2950-24	产品类型: 工作组级,二层,可网管型交换机,快速以太网交换机,背板带宽: 8.8 Gbps, 包转发率: 3.6Mpps, 传输方式: 存储转发方式	2	2450/1 台
PC 机	PC-TC	CPU 频率: 3.6GHz, 核心/线程数: 四核心/八线程, 内存容量 8GB, 硬盘容量 1TB, 独立显卡, 显存容量 2GB, 显示器尺寸 20 英寸	800	7000/台
直通线		产品适用:布线网络,最大单端长度: 100 米,提供基于 100MHz 带宽环境下的数据,传输速率为		4 元/m

		100Mbps		
DCE 串口线		用来同步时钟频率	-	-

（1）路由器：2811 隶属于 Cisco 2800 系列产品，与相似价位的前几代思科路由器相比，Cisco 2800 系列的性能提高了五倍、安全性和话音性能提高了十倍、具有全新内嵌服务选项，且大大提高了插槽性能和密度，同时保持了对目前 Cisco 1700 系列和 Cisco 2600 系列中现有 90 多种模块中大多数模块的支持，从而提供了极大的性能优势。2811 硬件结构图如图 3.4 所示。

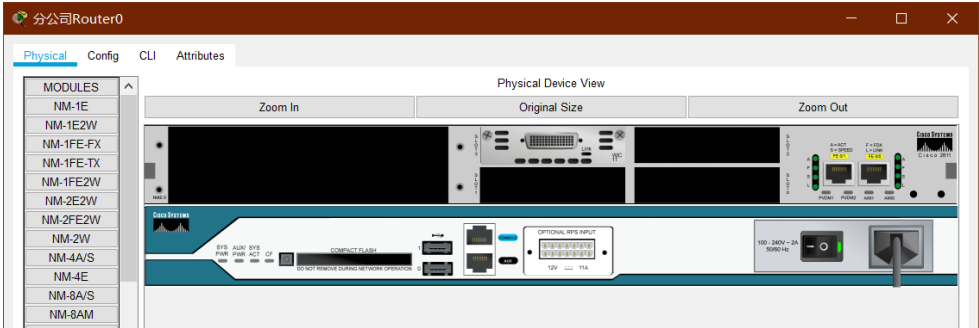


图 3.6 2811 分公司 Router0

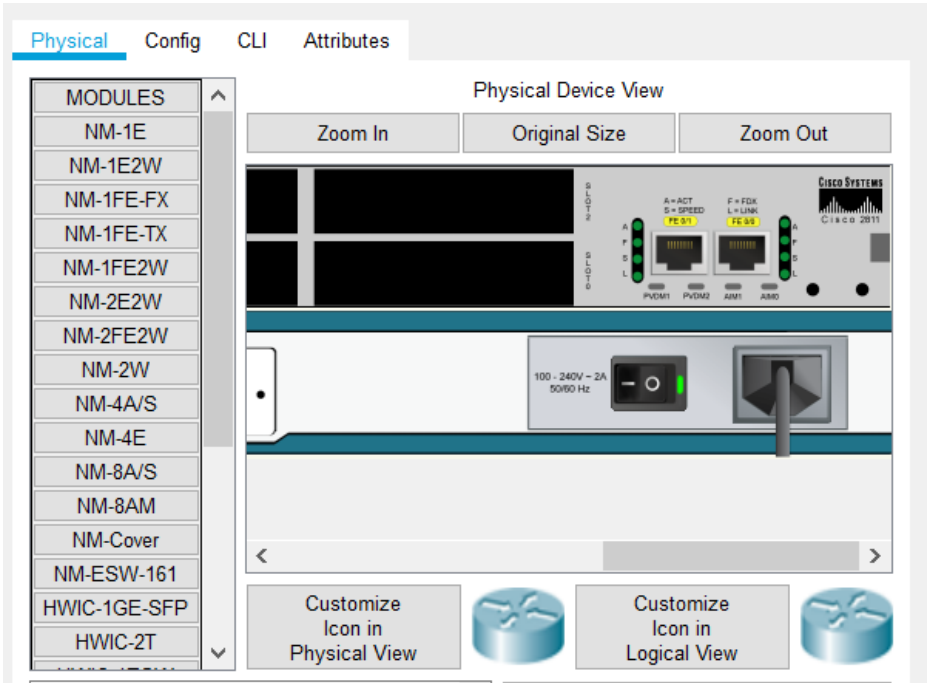


图 3.7 2811 路由器硬件结构图

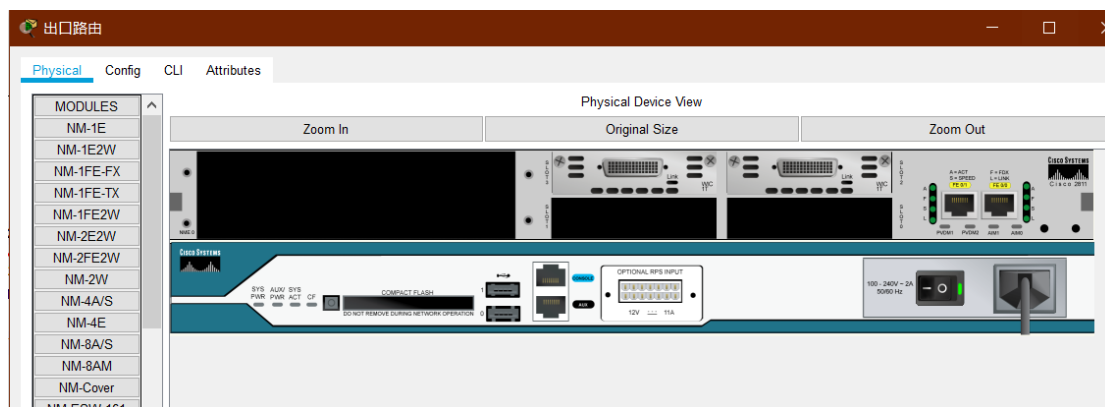


图 3.8 出口路由需要自行配置两个 Serial 口

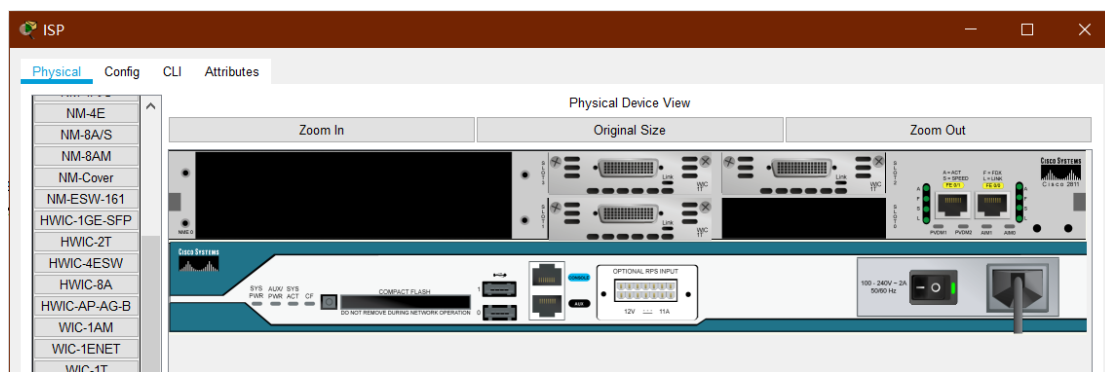


图 3.9 ISP 路由自行配置三个 Serial 口

(2) 交换机：CISCO WS-C3560-24PS 是企业级交换机，应用层级为三层。提供了可用性、安全性和服务质量功能，改进了网络运营，采用 24 端口配置，配备 2 个模块化插槽，接口丰富。还支持堆叠功能，扩展性十分强大，功能比较丰富。Cisco Catalyst 2950 系列智能以太网交换机是一个固定配置、可堆叠的独立设备系列，提供了快速以太网和千兆位以太网连接，凭借内置 Cisco 集群管理套件可出色地管理并轻松地配置第 2-4 层服务。思科 WS-C2960-24TC-L 企业级智能交换机是 2960 系列中的佼佼者，实现全新、独立的固定配置设备，拥有 24 个以太网接口，包含所提供的 10/100 快速以太网和 10/100/1000 千兆以太网边缘智能交换功能，对 LAN 服务功能有一定的增强作用，方便网络管理员对其进行管理同时可以使用铜缆或光纤上行链路。使用多种交换机体现了物理层兼容性。

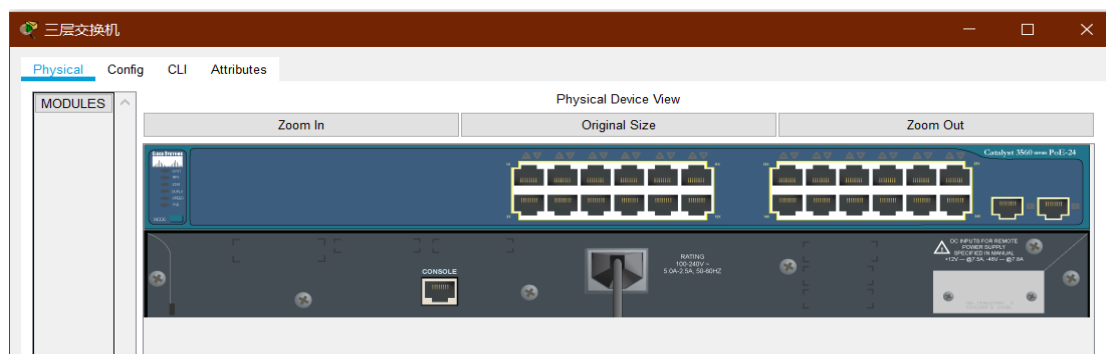


图 3.10 3560-24ps 三层交换机

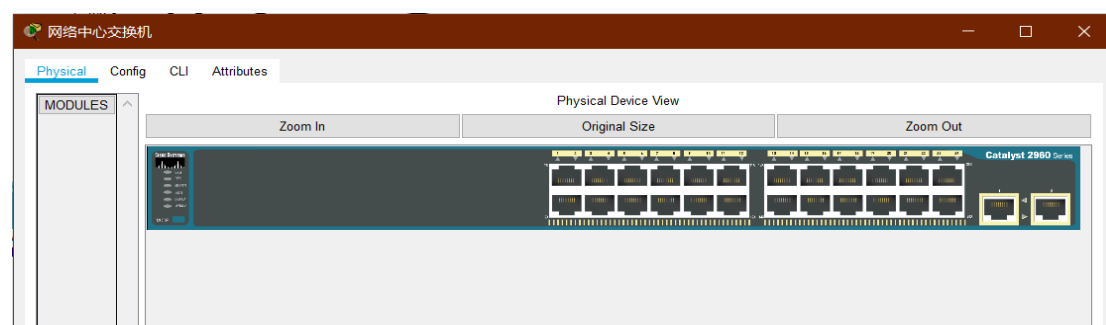


图 3.11 2960-2TT 网络中心交换机

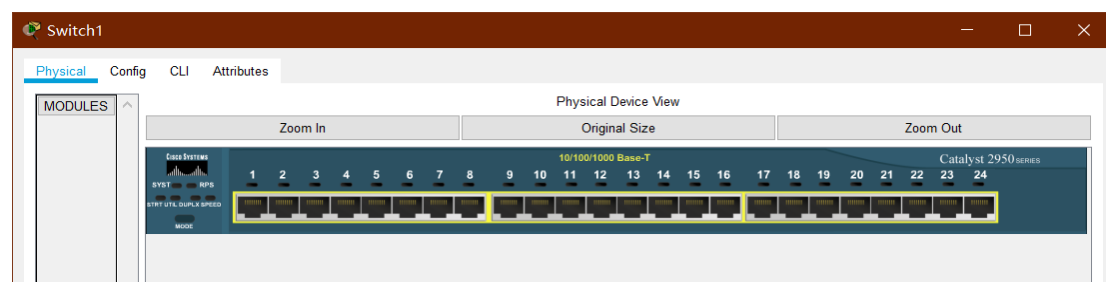


图 3.12 2950-24Switch

(3) 服务器：服务器比普通计算机运行更快、负载更高、价格更贵。服务器在网络中为其它客户机（如 PC 机、智能手机、ATM 等终端甚至是火车系统等大型设备）提供计算或者应用服务。服务器具有高速的 CPU 运算能力、长时间的可靠运行、强大的 I/O 外部数据吞吐能力以及更好的扩展性。根据服务器所提供的服务，一般来说服务器都具备承担响应服务请求、承担服务、保障服务的能力。服务器作为电子设备，其内部的结构十分的复杂，但与普通的计算机内部结构相差不大，如：CPU、硬盘、内存，系统，系统总线等。

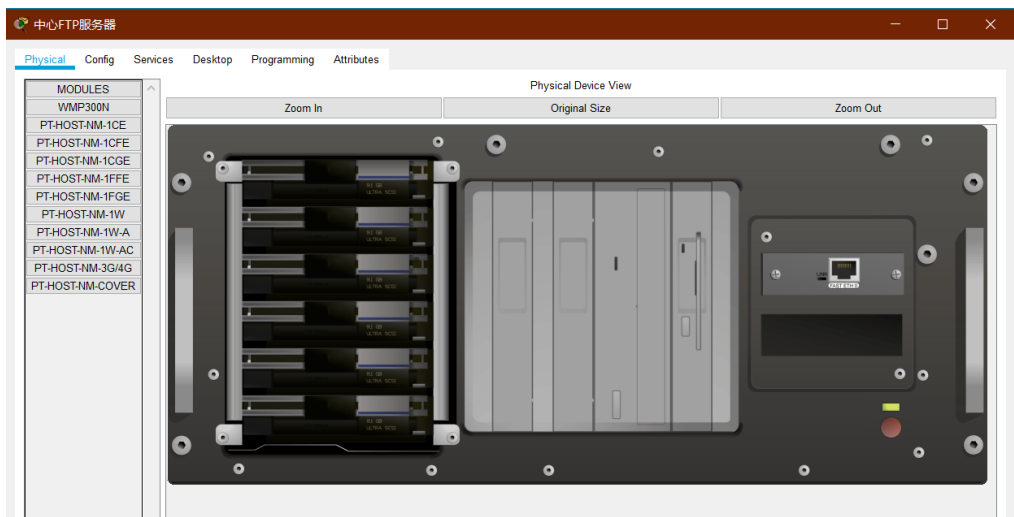


图 3.13 中心 FTP 服务器硬件结构图

3.3 地址规划

IP 地址规划方法^[7]有许多，在本课程设计中，使用无分类的 IP 地址。本公司需要支持 800 台 PC 同时使用，于是对于每一个 VLAN，都划分了 254 个 IP 地址（网络地址和广播地址除外），既满足了基本的需求，也考虑到了后续公司发展的扩展性，满足更多的 PC 要加入这个 VLAN 中。

表 3.2 VLAN 地址规划表

部门名称	VLAN	IP 网段	默认网关
网络中心	VLAN80	192.168.8.0/24	192.168.8.1/24
部门一	VLAN10	192.168.1.0/24	192.168.1.1/24
部门二	VLAN20	192.168.2.0/24	192.168.2.1/24
部门三	VLAN30	192.168.3.0/24	192.168.3.1/24
部门四	VLAN40	192.168.4.0/24	192.168.4.1/24
部门五	VLAN50	192.168.5.0/24	192.168.5.1/24
部门六	VLAN60	192.168.6.0/24	192.168.6.1/24
部门七	VLAN70	192.168.7.0/24	192.168.7.1/24
服务器集群	VLAN80	192.168.8.0/24	192.168.8.1/24
部门八	VLAN14	192.168.14.0/24	192.168.14.1/24

表 1.3 服务器地址规划表

设备名称	IP 地址	子网掩码	网关
外部 PC	172.17.0.10	255.255.0.0	172.17.0.1
外部服务器 A	172.17.0.11	255.255.0.0	172.17.0.1
外部服务器 B	172.17.0.12	255.255.0.0	172.17.0.1
DNS 服务器	192.168.8.10	255.255.255.0	192.168.8.1
DHCP 服务器	192.168.8.11	255.255.255.0	192.168.8.1
Web 服务器 a	192.168.8.12	255.255.255.0	192.168.8.1
Web OA 服务器	192.168.8.2	255.255.255.0	192.168.8.1

在如下表所示的 VLAN pool 中，有设置最大用户数的字段，由于目前公司支持 800 台 PC，所以最大用户数设置为 100，当公司的规模扩展，这里的最大用户数可以最大到 256。

表 3.4 DHCP 中 VLAN pool 的配置

Pool Name	默认网关	起始 IP 地址	最大用户数
VLAN60	192.168.6.1	192.168.6.20	100
VLAN50	192.168.5.1	192.168.5.20	100
VLAN40	192.168.4.1	192.168.4.20	100
VLAN30	192.168.3.1	192.168.3.20	100
VLAN20	192.168.2.1	192.168.2.20	100
VLAN10	192.168.1.1	192.168.1.20	100
server pool	0.0.0.0	192.168.8.0	256

3.4 网络设备配置

(1) 网络集群交换机的配置^{[8][10]}

这里使用 VLAN80 作为例子，对于 f0/2 到 f0/24 的所有端口，都设置端口模式为 access，端口对应于 VLAN80，对于 fa0/1 设置端口模式为 Trunk。

```
Switch(config)#vlan 80
```

```
Switch(config-vlan)#exit
Switch(config)#int range f0/2-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 80
Switch(config-if-range)#exit
Switch(config)#int f0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
```

(2) 三层交换机配置^[12]

对于在 Fa0/2 到 Fa0/6 的所有端口, 设置端口模式为 Trunk, 设置端口为 dot1q 封装且允许所有的 VLAN。

```
Switch(config)#interface range FastEthernet0/2-5
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport trunk allowed vlan all
Switch(config)#interface range FastEthernet0/6
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
```

(3) VLAN 划分配置^[11] (以一个为例)

VLAN 的划分只需要直接输入 vlan10 就可以新建一个 VLAN

```
Switch(config-if-range)#exit
Switch(config)#vlan 10
Switch(config-vlan)#exit
```

(4) 三层路由 DHCP^[15]中继配置

在三层路由中，这里只使用了 VLAN10,VLAN20, VLAN30, VLAN40 为例，设置他们的 helper-address 作为 192.168.8.11。

```
Switch(config)#interface vlan 10
Switch(config-if)#ip helper-address 192.168.8.11
Switch(config-if)#exit
Switch(config)#interface vlan 20
Switch(config-if)#ip helper-address 192.168.8.11
Switch(config-if)#exit
Switch(config)#interface vlan 30
Switch(config-if)#ip helper-address 192.168.8.11
Switch(config-if)#exit
Switch(config)#interface vlan 40
Switch(config-if)#ip helper-address 192.168.8.11
Switch(config-if)#exit
```

(5) 有关 VPN 配置

对于出口路由设置入口 ip 和出口 ip,设置路由器不关闭模式。

```
Router>enable
Router#config t
Router(config)#host 出口路由
出口路由(config)#int fa0/0
出口路由(config-if)#ip add 192.168.10.1 255.255.255.0
出口路由(config-if)#no shut
出口路由(config-if)#exit
出口路由(config)#int fa0/1
出口路由(config-if)#ip address 172.16.0.1 255.0.0.0
出口路由(config-if)#no shut
```

对于 R2 进行初始化配置，设置出口路由和入口路由 ip 地址，并且设置为不关闭模式。

CONFIGURATION ON ROUTER R2:

```
Router>enable
Router#config t
Router(config)#host r2
r2(config)#int fa0/0
r2(config-if)#ip add 172.16.0.2 255.0.0.0
r2(config-if)#no shut
r2(config-if)#exit
r2(config)#int fa0/1
r2(config-if)#ip add 172.15.0.1 255.0.0.0
r2(config-if)#no shut
```

对于 R3 进行初始化配置，设置出口路由和入口路由 ip 地址，并且设置为不关闭模式。

CONFIGURATION ON ROUTER r3:

```
Router>enable
Router#config t
Router(config)#host r3
r3(config)#int fa0/0
r3(config-if)#ip add 172.15.0.2 255.0.0.0
r3(config-if)#no shut
r3(config-if)#exit
r3(config)#int fa0/1
r3(config-if)#ip add 192.168.7.1 255.255.255.0
r3(config-if)#no shut
```

DEFAULT ROUTING CONFIGURATION ON ROUTER 出口路由:

对于出口路由设置静态路由表

出口路由>enable

出口路由#config t

Enter configuration commands, one per line. End with CNTL/Z.

出口路由(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.2

出口路由(config)#

DEFAULT ROUTING CONFIGURATION ON ROUTER r3:

对于 R3 设置静态路由表

r3>enable

r3#config t

Enter configuration commands, one per line. End with CNTL/Z.

r3(config)#ip route 0.0.0.0 0.0.0.0 172.15.0.1

r3(config)#

出口路由设置 tunnel

设置 tunnel，tunnel 的 ip 地址和出发端口，目的 ip 地址

出口路由#config t

出口路由(config)#interface tunnel 10

出口路由(config-if)#ip address 10.10.1.2 255.255.0.0

出口路由(config-if)#tunnel source fa0/1

出口路由(config-if)#tunnel destination 172.15.0.2

出口路由(config-if)#no shut

R3 设置 tunnel

同样的，对于另一端的设置 tunnel 的 ip 地址和出发端口，目的 ip 地址

r3#config t

r3(config)#interface tunnel 100

```
r3(config-if)#ip address 10.10.1.1 255.255.0.0
r3(config-if)#tunnel source fa0/0
r3(config-if)#tunnel destination 172.16.0.1
r3(config-if)#no shut
```

(6) 出口路由 NAT

设置出口路由的 NAT， access-list 允许的 ip 地址， natpool 以及 netmask

```
Router(config)#access-list 101 permit ip 192.168.0.0 0.0.255.255 any
Router(config)#access-list 101 permit tcp any 192.168.8.11 0.0.0.0
Router(config)#ip nat pool pool-1 172.16.1.0 172.16.2.255 netmask 255.255.0.0
Router(config)#ip nat inside source list 101 pool pool-1 overload
Router(config)#interface FastEthernet0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface Serial0/3/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

(7) 出口路由默认配置

```
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.2
```

(8) 静态 NAT^[14]映射，外网可以访问网络中心服务器

```
Router(config)#ip nat inside source static 192.168.8.12 172.16.1.11
```

(9) 交换机配置信息

下表中的 Trunk 的含义为端口聚合，Trunk 实现了相同 VLAN 不需要跨越不同交换机 VLAN 内的主机之间的直接通信。在实际的设置中，只要是交换机和

交换机相连接的端口都设为 Trunk, 对于交换机和 PC 相连接的端口设置为 Access。

表 3.5 交换机配置信息

交换机名称	型号	Fa0/1	Fa0/2	Fa0/3	Fa0/4
部门一交换机	2960-24TT	Trunk	Access, VLAN10	Access,VLAN 10	Access,VLAN10	
部门二交换机	2960-24TT	Trunk	Access, VLAN20	Access,VLAN 20	Access,VLAN20	
部门三交换机	2960-24TT	Trunk	Access, VLAN30	Access,VLAN 30	Access,VLAN30	
部门四交换机	2960-24TT	Trunk	Access, VLAN40	Access,VLAN 40	Access,VLAN40	
部门五交换机	2960-24TT	Trunk	Access, VLAN50	Access,VLAN 50	Access,VLAN50	
部门六交换机	2960-24TT	Trunk	Access, VLAN60	Access,VLAN 60	Access,VLAN60	
部门七交换机	2960-24TT	Trunk	Access, VLAN70	Access,VLAN 70	Access,VLAN70	
部门八交换机	2960-24TT	Trunk	Access, VLAN140	Access,VLAN 14	Access,VLAN14	
网络中心交换机	2960-24TT	Trunk	Access, VLAN80	Access,VLAN 80	Access,VLAN80	
外部交换机	2960-24TT	Access	Access	Access	Access	
三层交换机	2560-24ps	Trunk	Trunk	Trunk	Trunk	

(10) 路由器配置信息

下表中 Fa 全称为 FastEthernet, S 全称为 Serial, 也就是串口, 对于每一个端口都需要配备出口 ip 和入口 ip。注意到在表中有 ip 地址重复的情况, 这是由于

使用了备份出口路由，备份出口路由的各项设置和出口路由设置完全相同，对于 ISP 连接的串口接出口路由 ip 和接备份出口路由 ip 也是相同的。

表 3.6 路由器配置信息

路由器名称	型号	Fa0/0	Fa0/1	Fa0/2	S0/0/0	S0/1/0	S0/2/0	S0/3/0
出口路由	2811	-	192.168.10.1	-	-	-	172.15.0.1	172.16.0.1	
分公司 Router0	2811	192.16.8.7.1	-	-	-	-	-	172.15.0.2	
分公司 Router1	2811	198.16.8.17.1	-	-	-	-	-	172.14.0.2	
备份出口路由	2811	-	192.168.10.1	-	-	-	172.15.0.1	172.16.0.1	
ISP	2811	172.17.0.1	-	-	172.16.0.2	172.15.0.1	172.15.0.2	172.16.0.2	

(11) 服务器配置

在 Cisco Packet Tracer 服务器的实现中，已经有很完整的应用层 FTP, DNS, HTTP, DHCP 等服务的封装，在使用对应的服务时，我们只需要在服务器上开启相关服务并进行网关，子网掩码配置，用户名密码创建即可，需要注意的是，对于已经实例化的服务器，需要将无关或者不用的服务关掉，以免与其他服务器产生冲突。

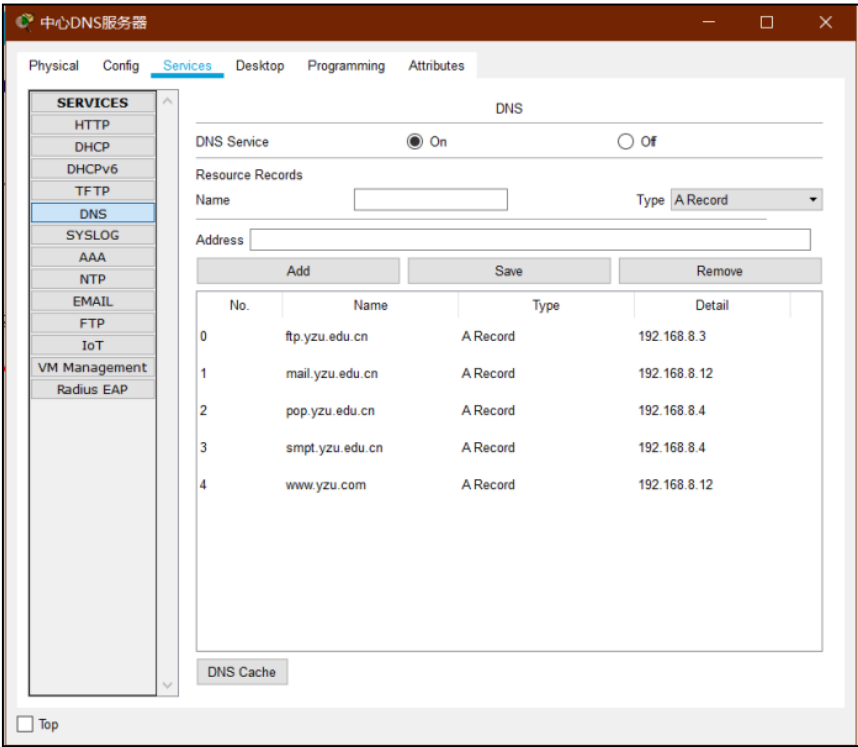


图 3.14 DNS 设置

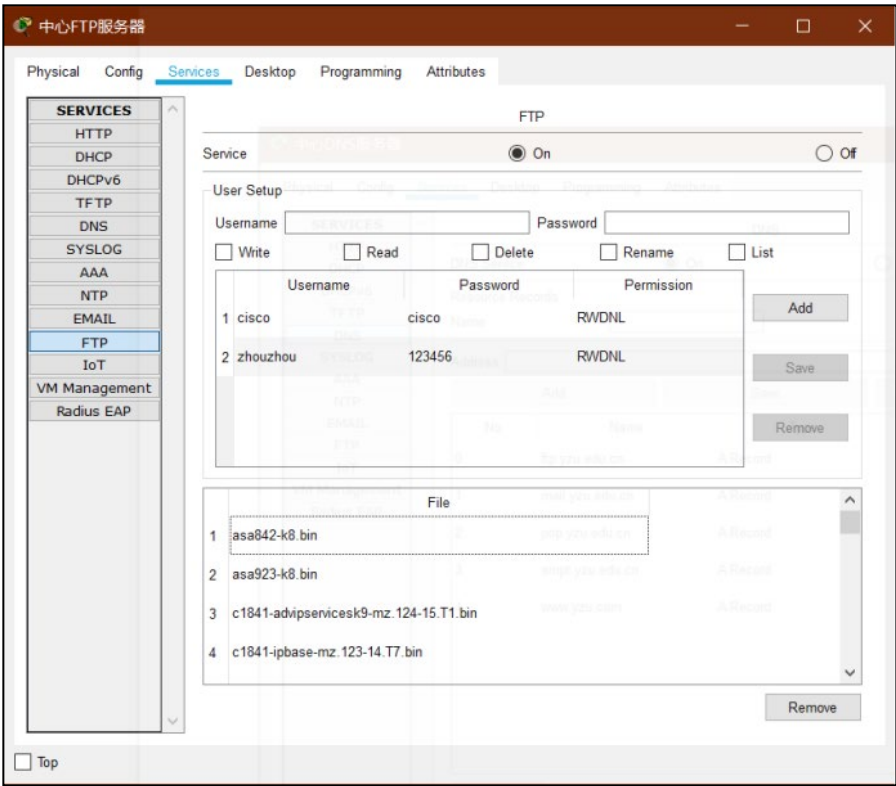


图 3.15 中心 FTP 服务器设置

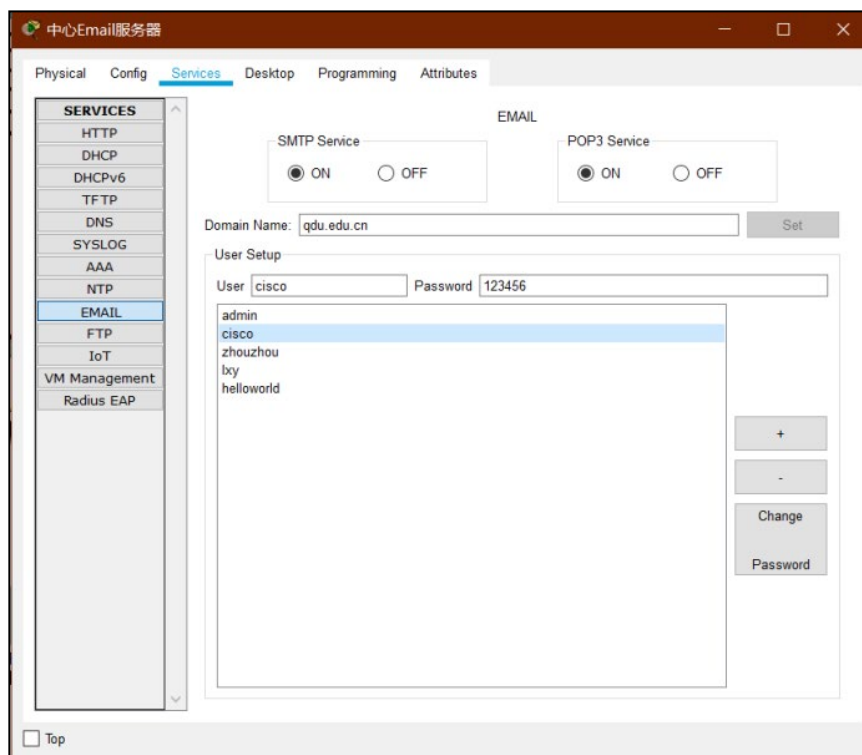


图 3.16 Email 服务设置

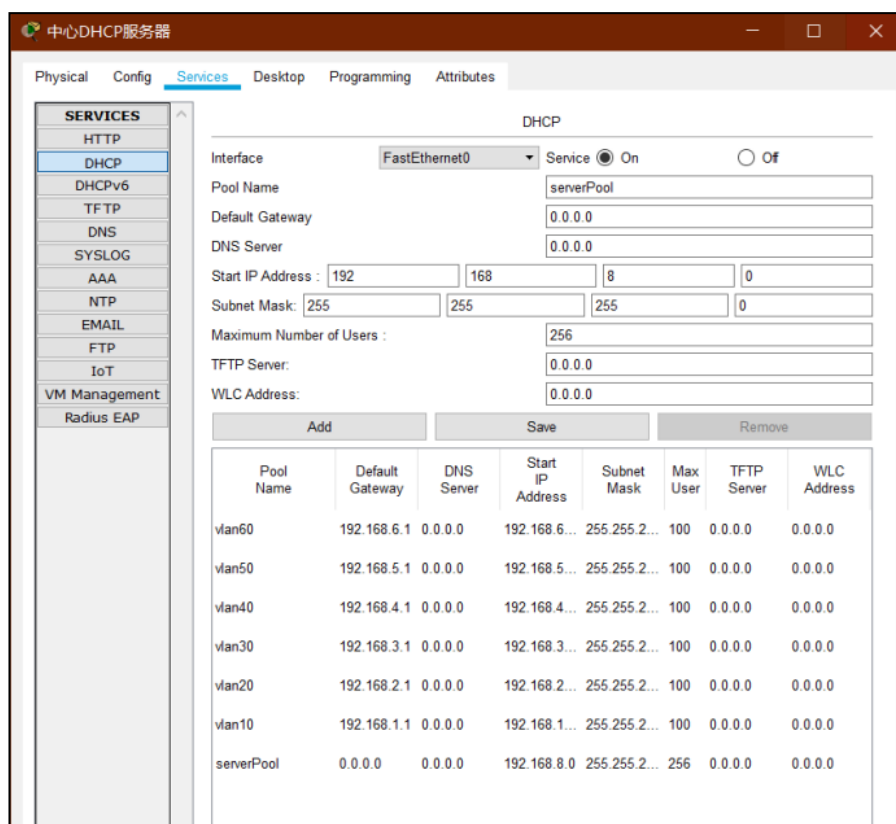


图 3.17 DHCP 服务设置

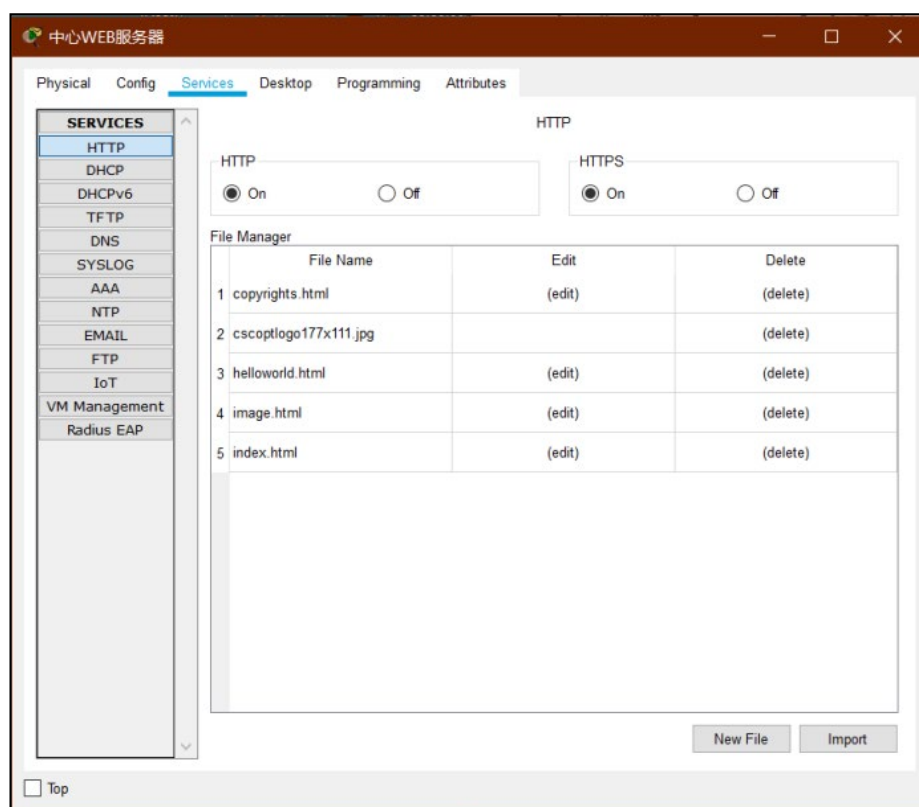


图 3.18 Web 服务设置

第 4 章 网络物理设计

根据相关协议或标准，进行标准化的网络综合布线设计。本章从物理层的角度出发，分析了传输介质选择的原因以及实际的综合布线设计。

4.1 传输介质选择

(1) 直通线：

在 Cisco Packet Tracer^[9]中用这个图标表示。



这是常见的 RJ45 标准的直通双绞线，不同设备之间相连常使用直通线。

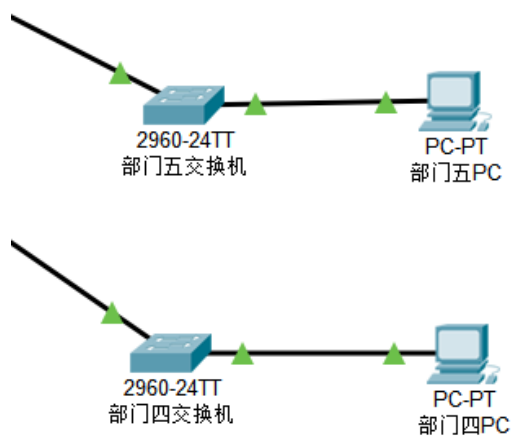


图 4.1 交换机和主机用直通线相连

(2) 串口线：

在 Cisco Packet Trace 中用这个图标表示。



这种 DCE 连接方式通常用在两个路由器之间的串口进行。

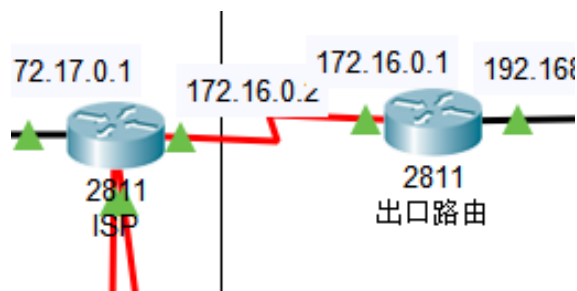


图 4.2 路由器之间用串口线相连

4.2 综合布线设计

4.2.1 总公司布线设计

总公司共有 6 个部门，采用直通线连接 6 个交换机。

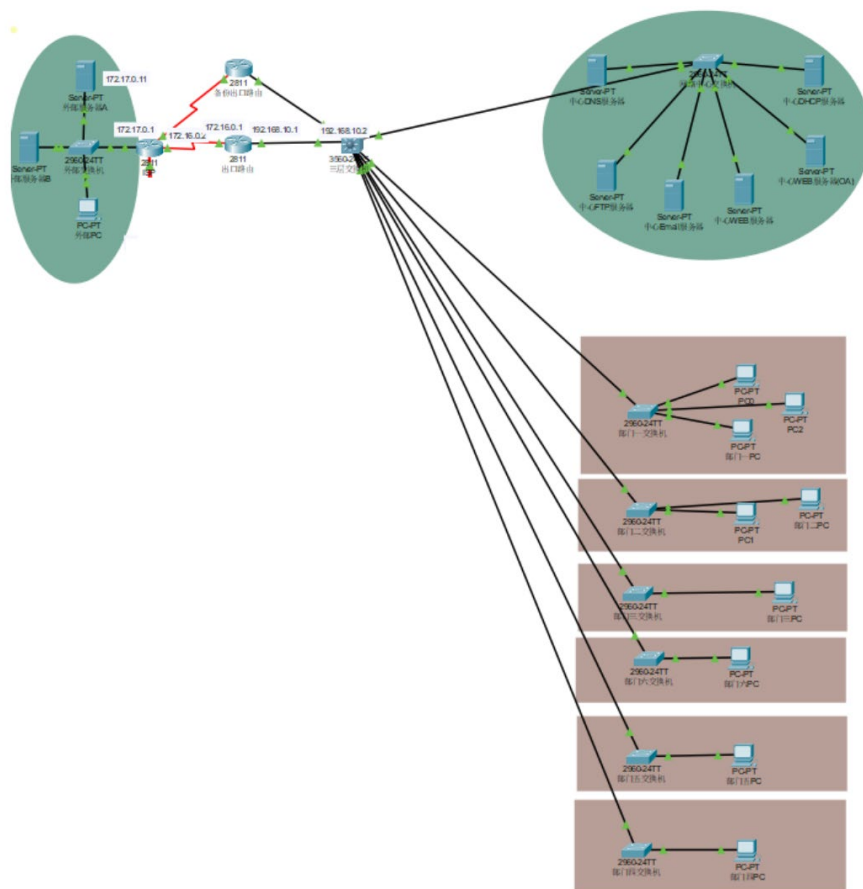


图 4.3 总公司布线设计

4.2.2 分公司布线设计

该公司有两个分公司，每个分公司有两个部门，每个路由器通过直通线与交换机相连，交换机再采用直通线连接主机。

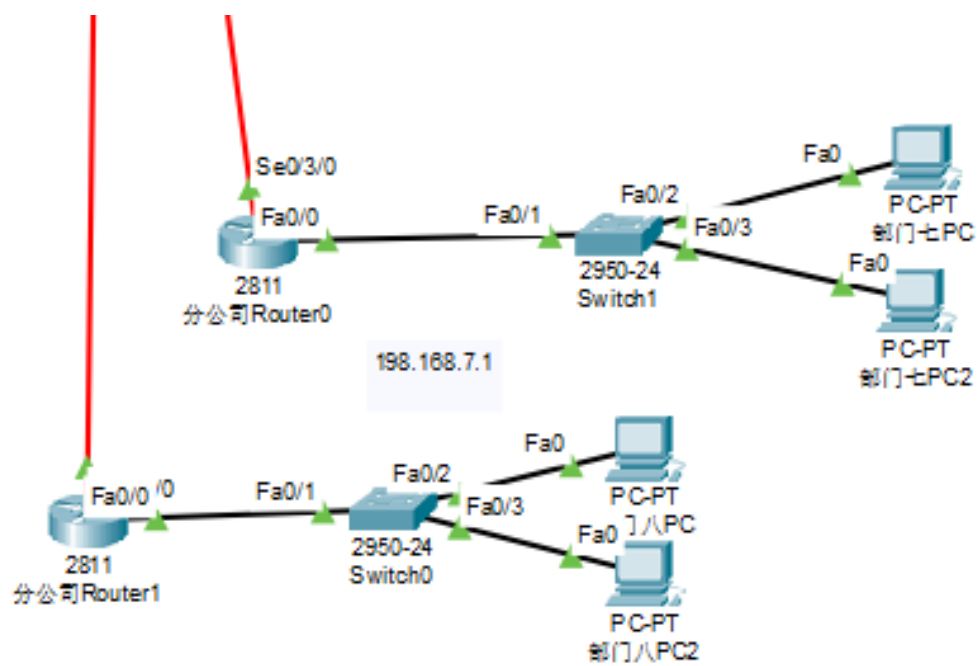


图 4.4 分公司布线设计

第 5 章 系统测试

系统测试的目的，一个是解决系统设计中的功能实现是否存在问题；二是解决各子系统间通信是否存在 Bug。测试方法主要有：单元测试、集成测试、系统测试，在单元测试的基础中进行集成测试，在集成测试的基础中进行系统测试。本章进行了详细全面的系统测试。测试主要分为两个方面，一个是连通性测试，一个是功能性测试，连通性测试顾名思义即查看是否网络能够正常访问，对于满足访问权限的情况是否正常访问对应的 ip，对于已经设定了访问限制的情况，这样的访问限制是否成功进行。功能性测试主要是测试有关功能是否达到预期的结构，比如说 mail 是否都能够正常发送，正常接收，公司的 OA 系统能够正常登录等等。

5.1 测试工具

5.1.1 ping 指令

在测试中，我们主要在 PC/服务器/交换机的终端（Terminal）中使用 ping 指令来对各种服务功能以及连通性进行测试，在网络中 ping 是一个十分强大的 TCP/IP 测试工具，通过使用 ping 指令，我们可以测试：

- （1）网络的连通情况和网络速度；
- （2）DNS 解析是否正确

5.1.2 cisco 模拟桌面

如下图所示，在 packet tracer 中，提供了很完整的 PC 功能模拟，使用“桌面”中的各种工具（如浏览器，邮件应用）就可以很方便地对各种服务进行测试。

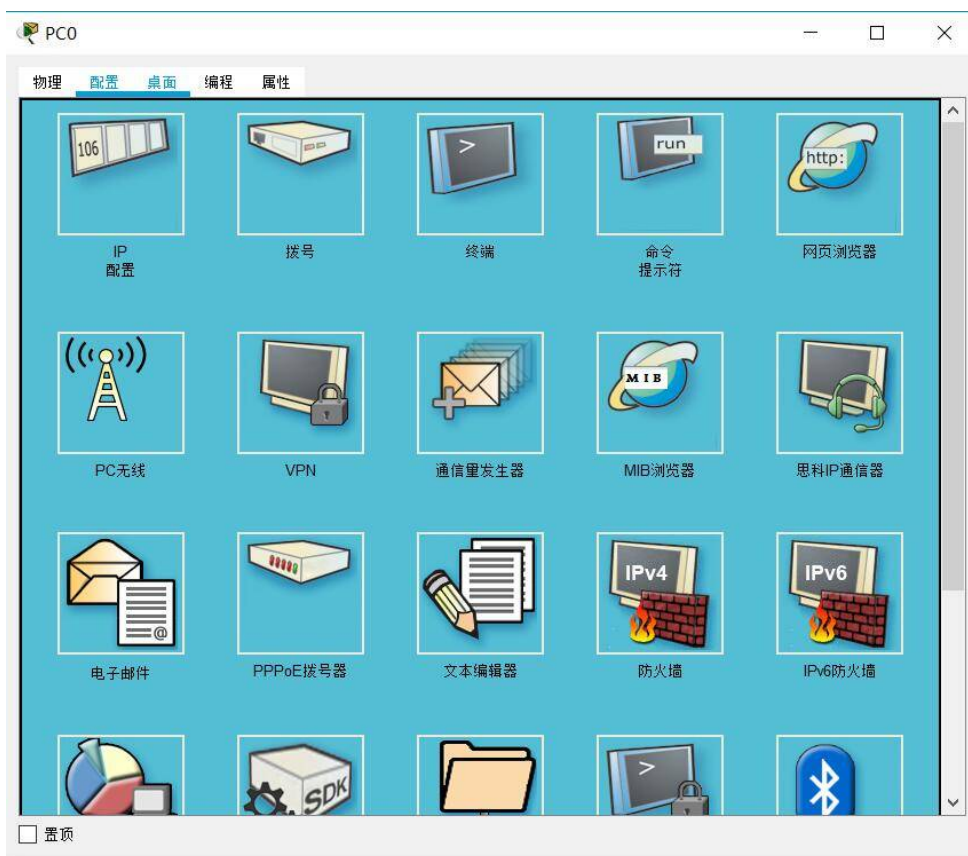


图 5.0 测试工具

5.2 有关服务器的连通性测试

5.2.1 外部服务器访问 PC 机的测试

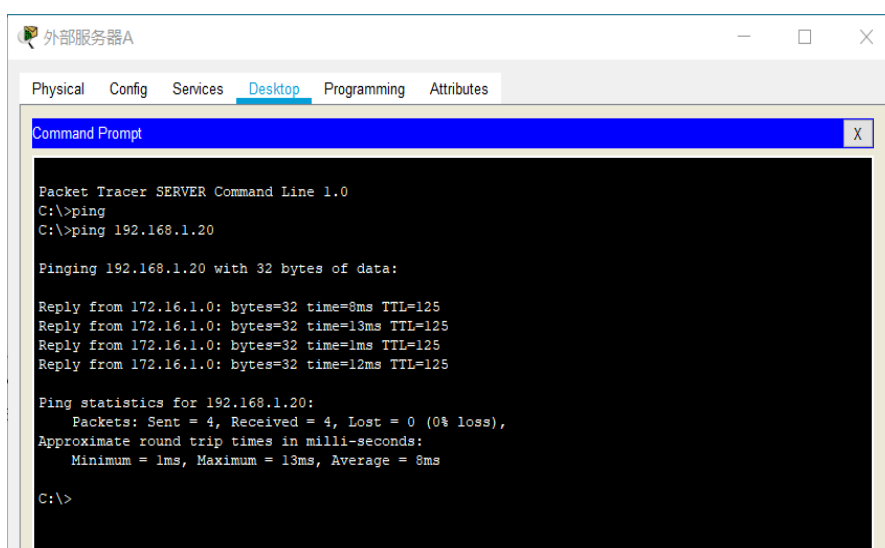


图 5.1 外部服务器 A ping 部门一的 PC1

对于部门二 PC, 由于访问限制的设置, 所以无法 ping 通, 显示 destination host unreachable

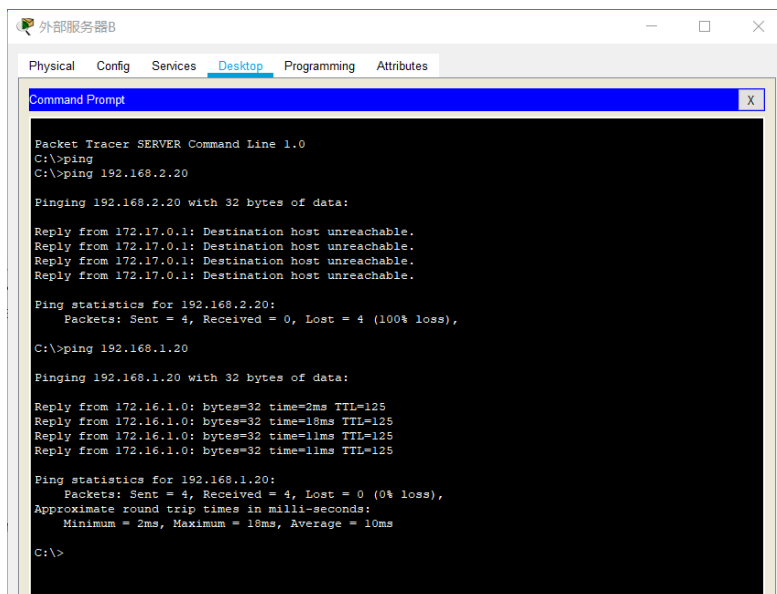


图 5.2 外部服务器 B ping 部门一 PC1

5.2.2 内部服务器访问 PC 机的测试

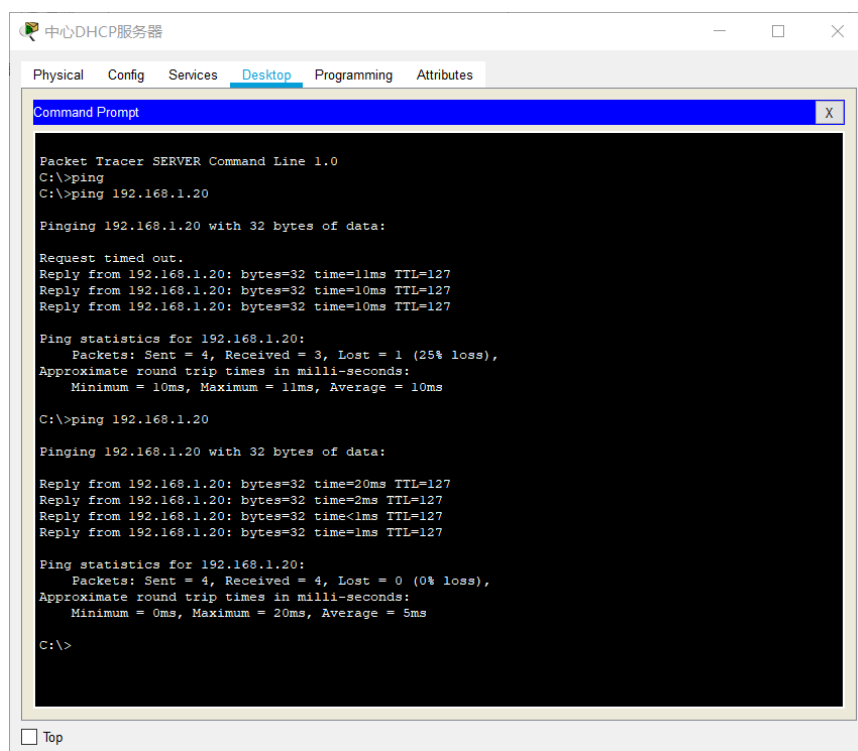


图 5.3 中心 DHCP 服务器访问部门一的 PC1 机

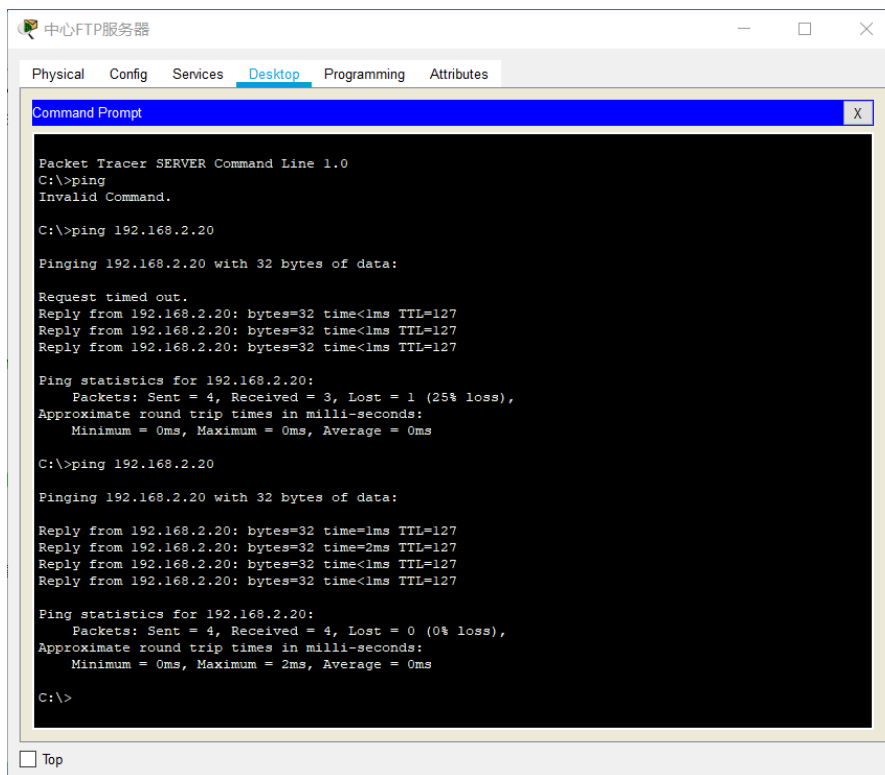


图 5.4 中心 FTP 服务器访问部门二的 PC1 机

5.2.3 外部服务器和内部服务器之间的连通性测试

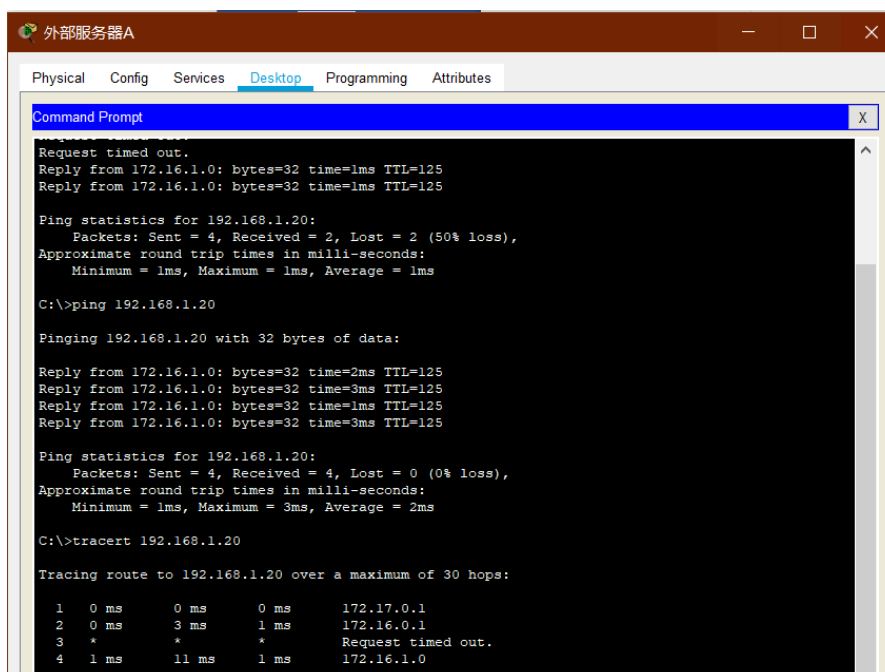


图 5.5 服务器 A Ping 服务器集群

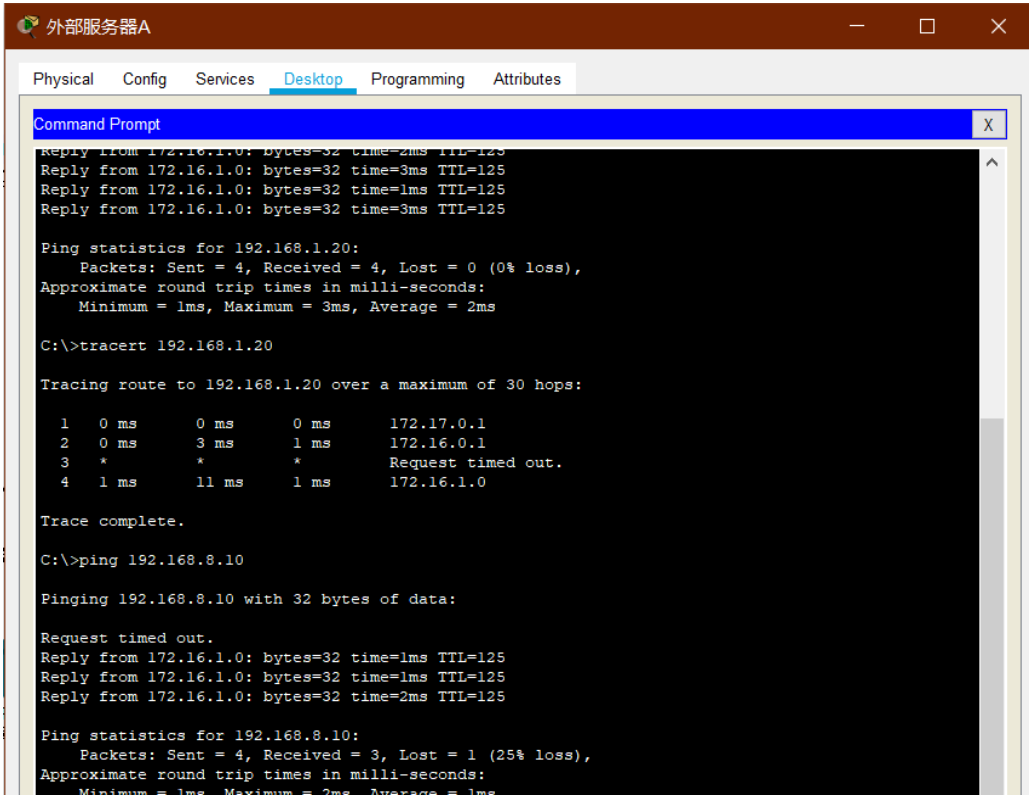


图 5.6 服务器 A Ping 服务器集群

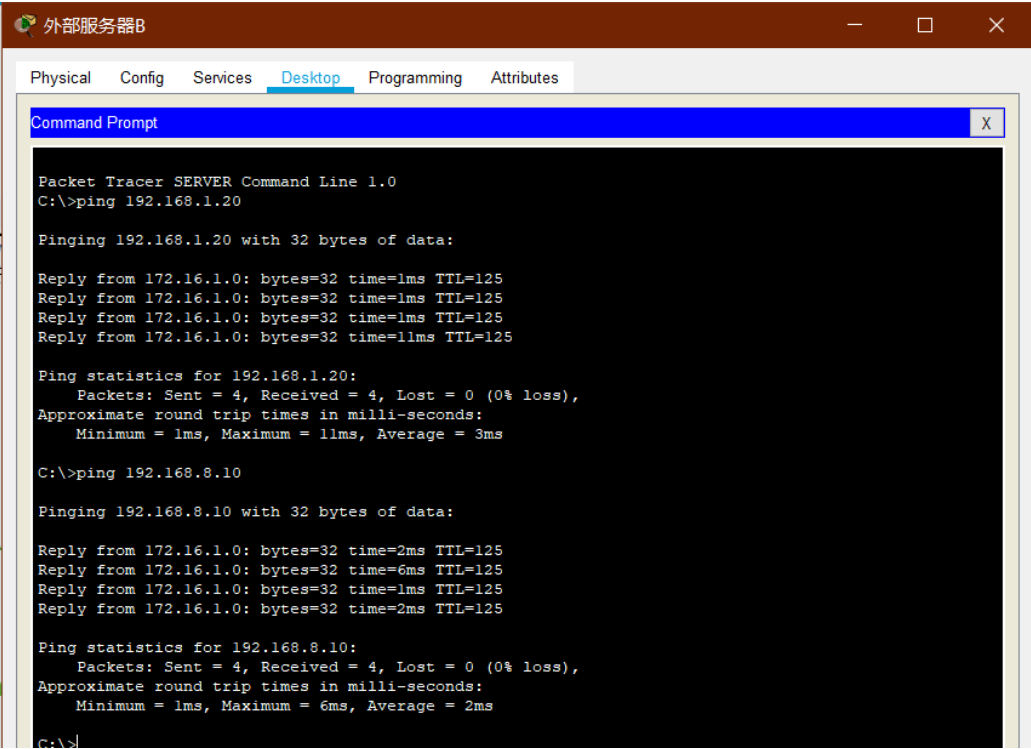


图 5.7 服务器 B Ping PC1 和服务器集群

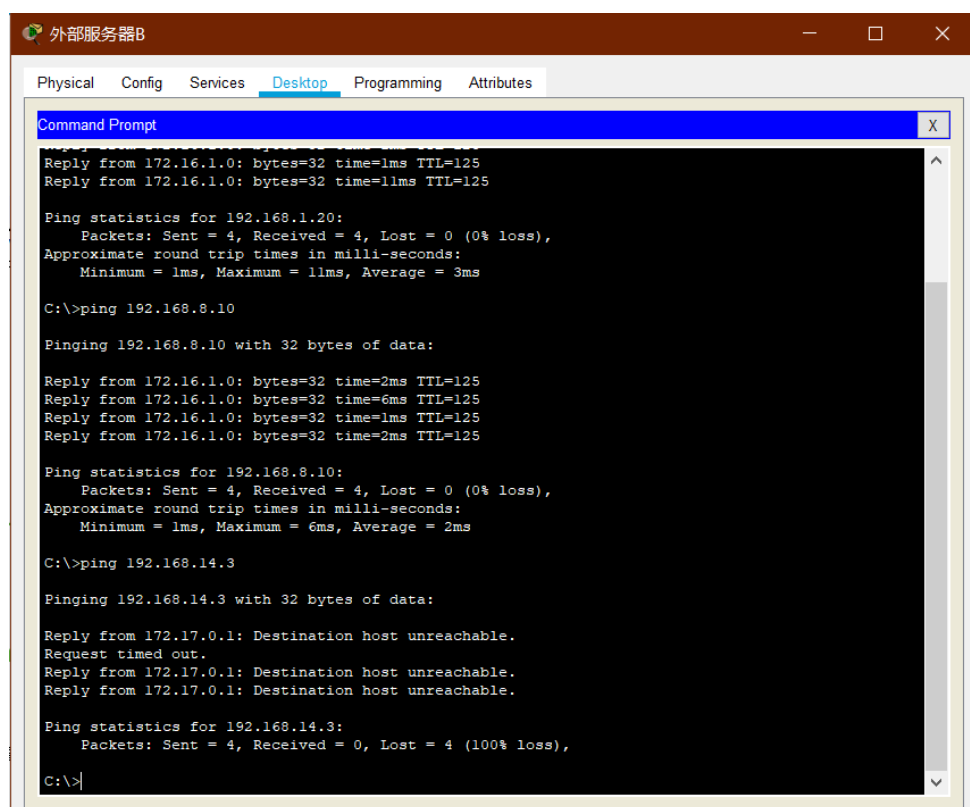


图 5.8 服务器 B Ping PC1 和服务器集群

5.3 PCi 与其它 PC 机的连通性测试

5.3.1 同一个 VLAN 之间 PC 连通性测试

PC0 和 PC1 位于同一个 VLAN 内，一个 ip 地址为 192.168.1.1，一个 ip 地址为 192.168.1.20，进行 ping,发现所有包都成功收到，ping 通。

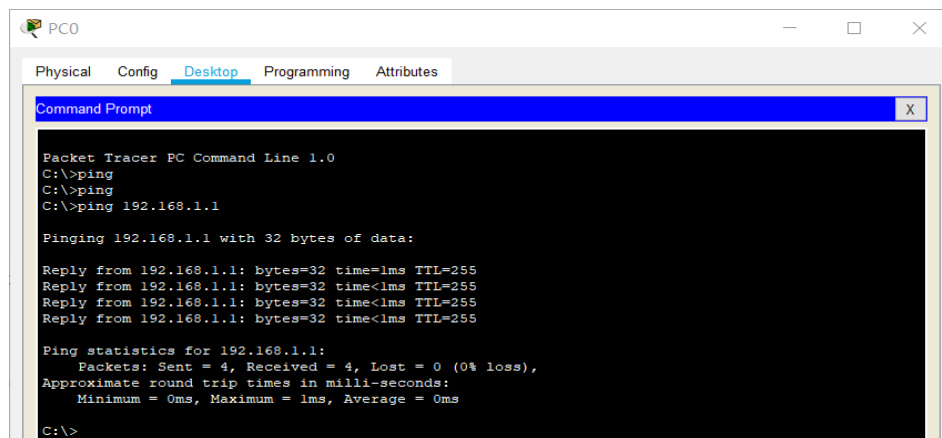


图 5.9 PC0 ping PC1

5.3.2 不同 VLAN 之间 PC 连通性测试

PC 和部门二 PC 位于不同 VLAN 内，一个 ip 地址为 192.168.1.20，一个 ip 地址为 192.168.2.20，进行 ping，发现所有包都成功收到，ping 通。

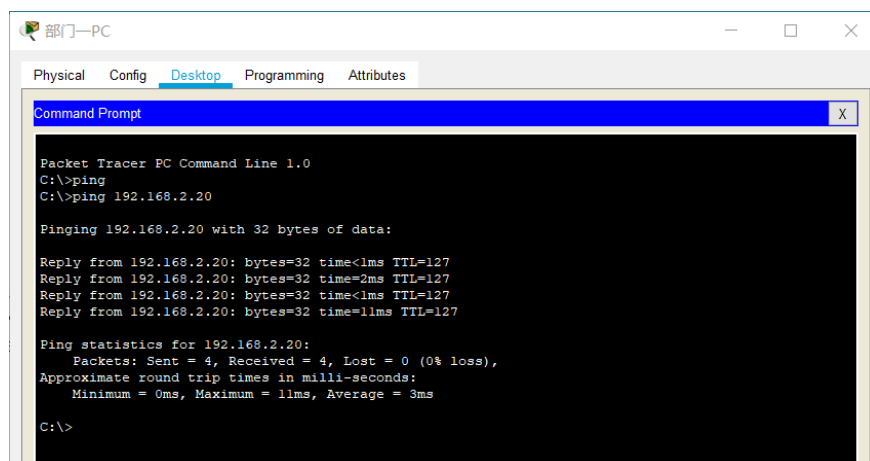


图 5.10 部门一 ping 部门二

5.3.3 分公司 PC 和总公司 PC 之间的连通性测试

部门七 PC 位于分公司，部门一 PC 位于总公司，ip 地址分别为 192.168.1.1，192.168.7.2，下图是分公司 PC ping 总公司 PC，第一次的时候丢包一个，第二次的时候没有丢包，全部收到，ping 通。

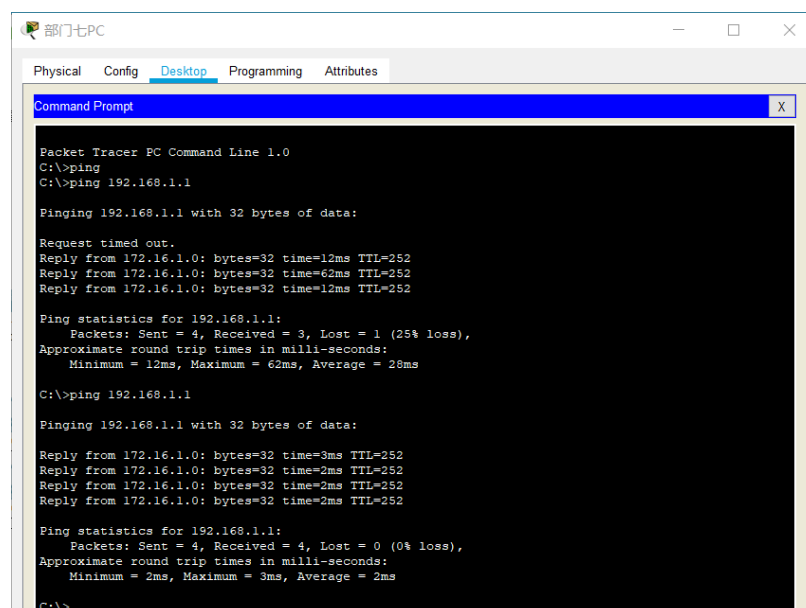


图 5.11 部门七 ping 部门一

部门七 PC 位于分公司，部门一 PC 位于总公司，ip 地址分别为 192.168.1.1，192.168.7.2，下图是总公司 PC ping 分公司 PC,没有丢包，全部收到，ping 通。

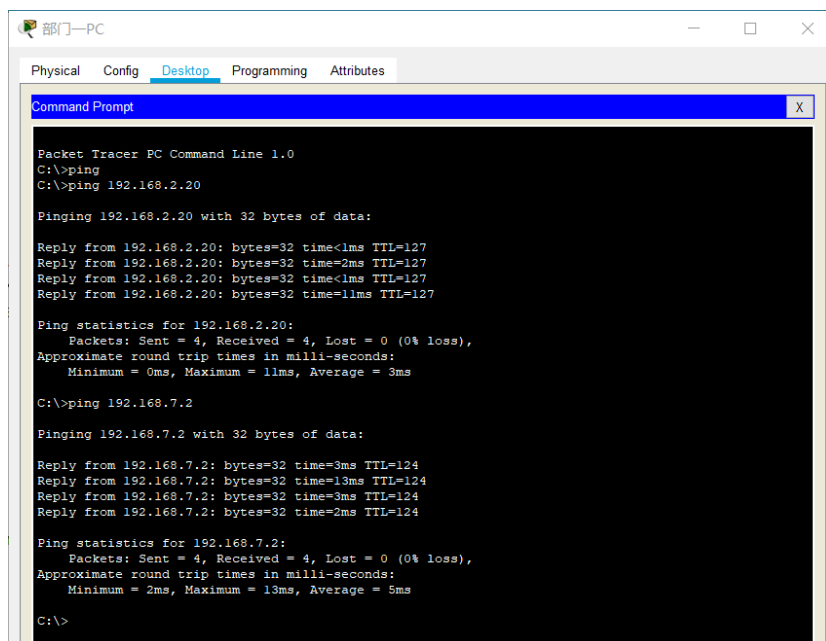


图 5.12 部门一 PC ping 分公司 PC

5.3.4 有关 VPN 的连通性测试

部门二 PC 和部门七 PC 位于 VPN 两边，在这里测试部门二 PC ping 部门七 PC,如果能够成功 ping 通，说明 VPN 所经过的链路通畅，路由正确。

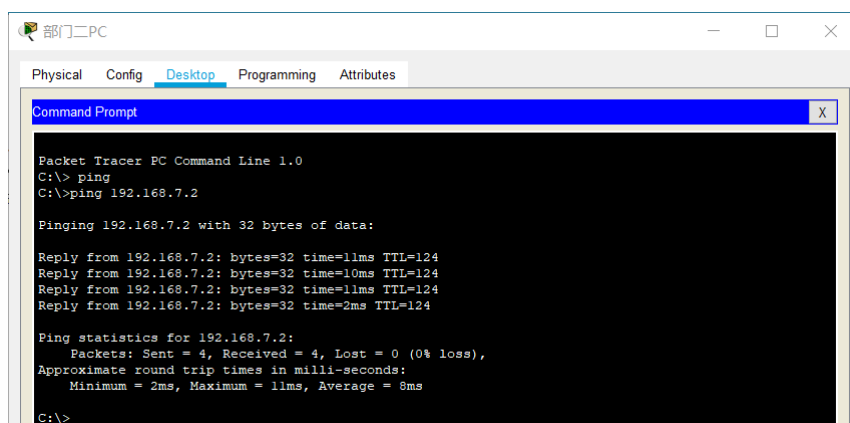


图 5.13 部门二 ping 部门七（说明 VPN 设置正确）

在分公司 Router0 上进行有关 ping，使用的是 VPN 的隧道地址 10.10.1.2，可以看到五个包都成功收到，进一步说明 VPN 隧道设置成功。

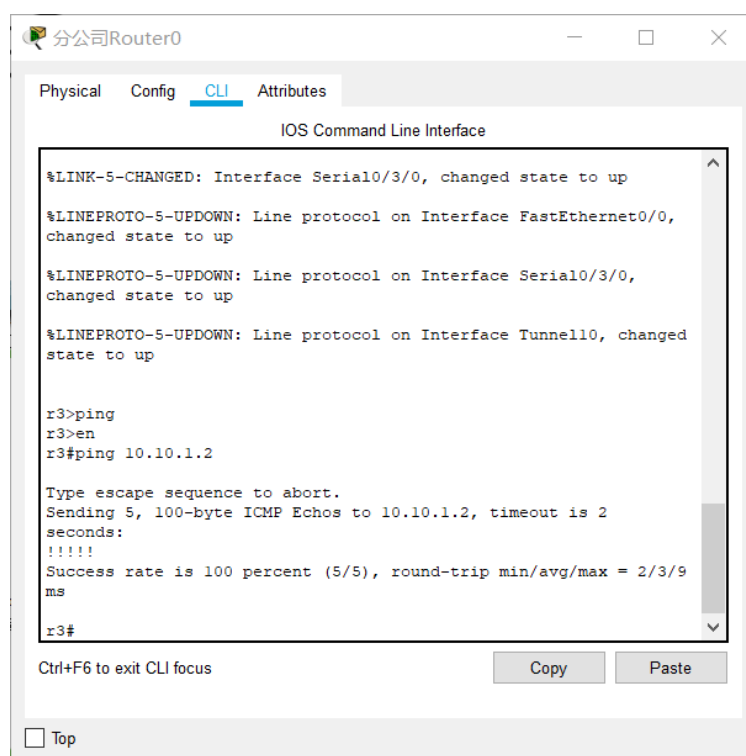


图 5.14 分公司 Router0 通过 VPN ping 出口路由

在出口路由，也就是 VPN 的另一个端口，进行 pingRouter0 的测试，这里 ping 的是隧道地址 10.10.1.1，五个包同样 ping 通，说明整个 VPN 都设置成功。

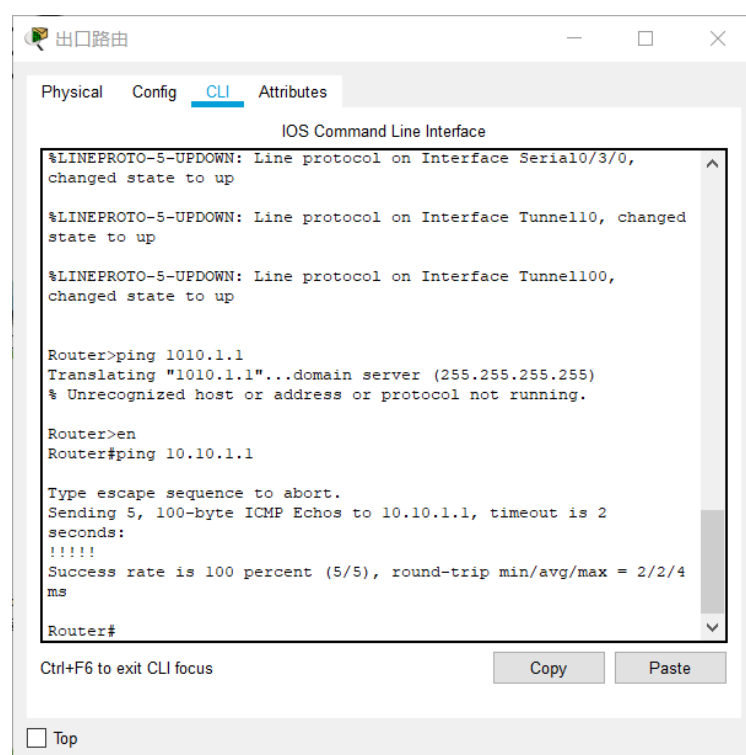


图 5.15 出口路由通过 VPN ping 分公司 Router0

在出口路由，也就是 VPN 的另一个端口，进行 pingRouter0 的测试，这里 ping 的是 Router0 的出口 ip172.16.0.1，五个包同样 ping 通，说明 VPN 都设置成功，有关路由正确设置。

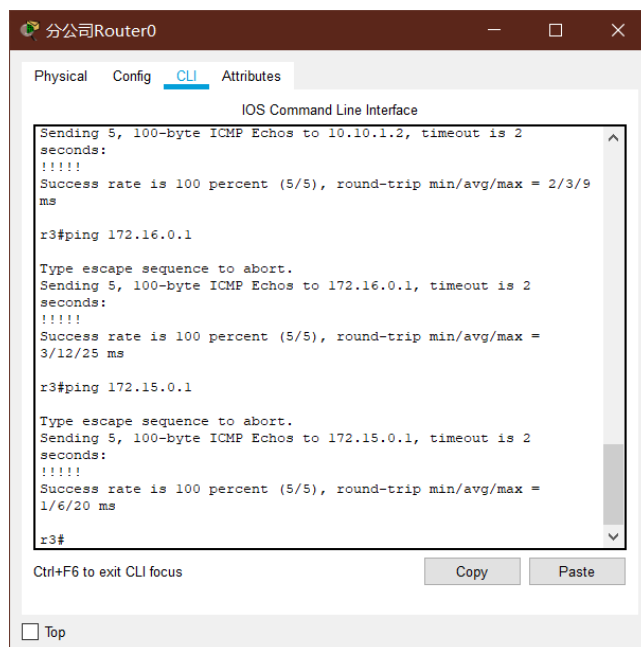


图 5.16 分公司 Router0 ping 出口路由的外部 IP 地址和 ISP 的外部 IP 地址

5.4 功能测试

5.4.1 web browser 测试

使用 web browser 进行访问内部网站，可以看到主页显示了该主页名称“扬大创新创业园”，<http://www.yzu.com/index.html>，说明 dns 解析正确。



图 5.17 web browser 进行访问内部网站

5.4.2 访问 OA 系统进行交互

由于 Cisco packet tracer 不支持 CSS, js 等前端, 我们只能使用 html 体现功能性, 可以看到此处是 OA 系统的登录界面, 有输入密码, 用户名登录 OA, 也有忘记密码的功能。

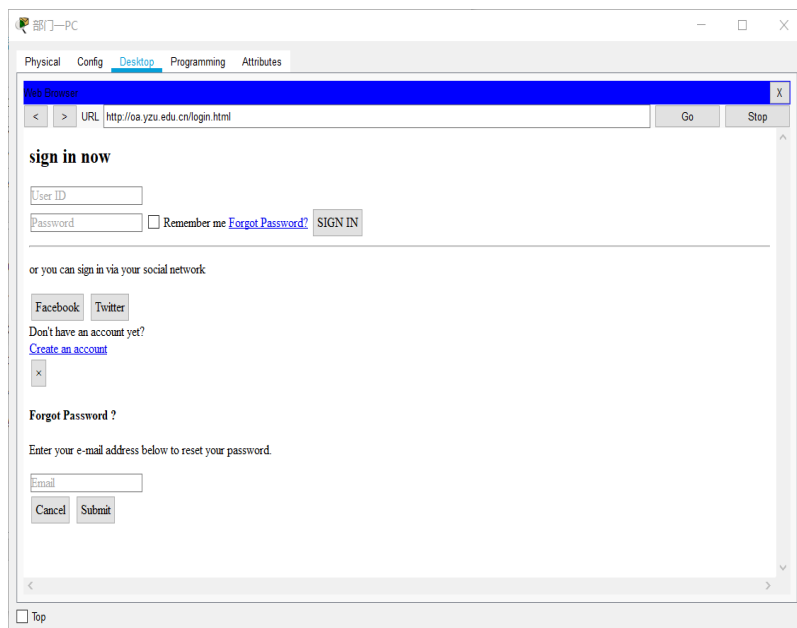


图 5.18 OA 系统登录界面

在登录到 OA 系统之后, 可以看到有 pending task 也就是待处理事项, new messages 也就是新收到的信息, 体现了 OA 系统功能的完备性。

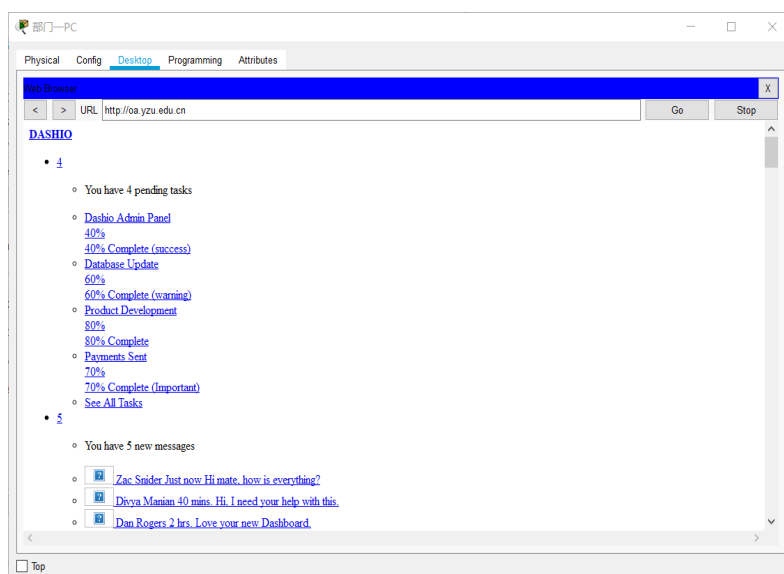


图 5.19 OA 系统中显示其他正办公的员工

OA 系统同样有显示当前正在办公的员工的功能，方便员工可以互相进行交流，避免打扰正在休假的员工。

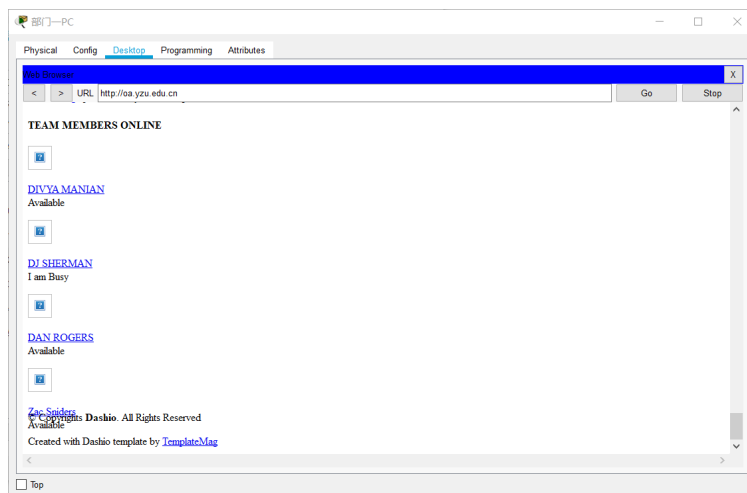


图 5.20 显示当前其他正在办公员工（OA）

5.4.3 FTP 服务测试

使用 ftp 服务，可以上传文件，查看文件。Cisco packet tracer 的 ftp 功能比较简陋，只支持 dir 和 put 功能，其他的一些常用功能都没有进行支持，可以看到在当前的主目录下已经有很多有关文件。

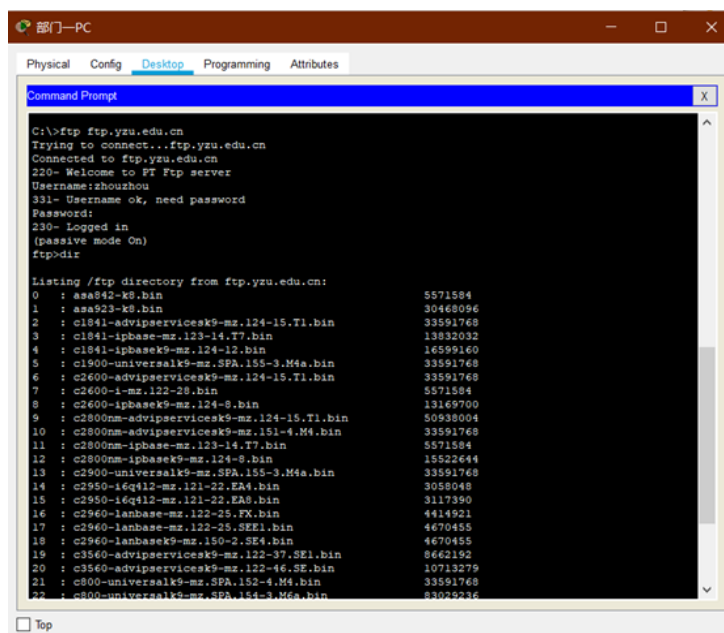


图 5.21 使用 ftp 服务

5.4.4 mail 服务测试

在部门一的 PC 上登录 mail 的账户，由于完善的配备了域名解析，有关的信息填写就非常易懂。

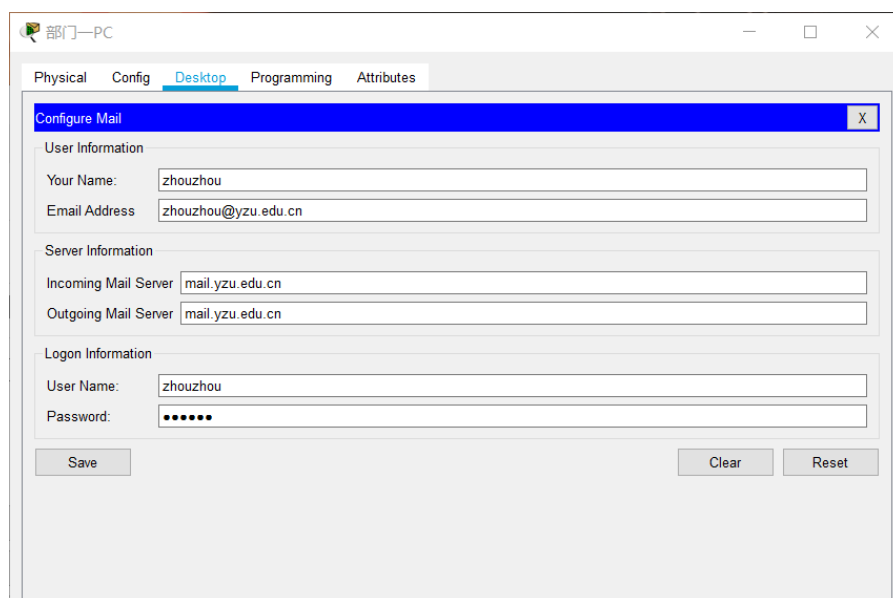


图 5.22 填写 mail 的账户信息

写收信人地址和主要内容，这里向 lxy 发送了一封主题为 hello world 的邮件。

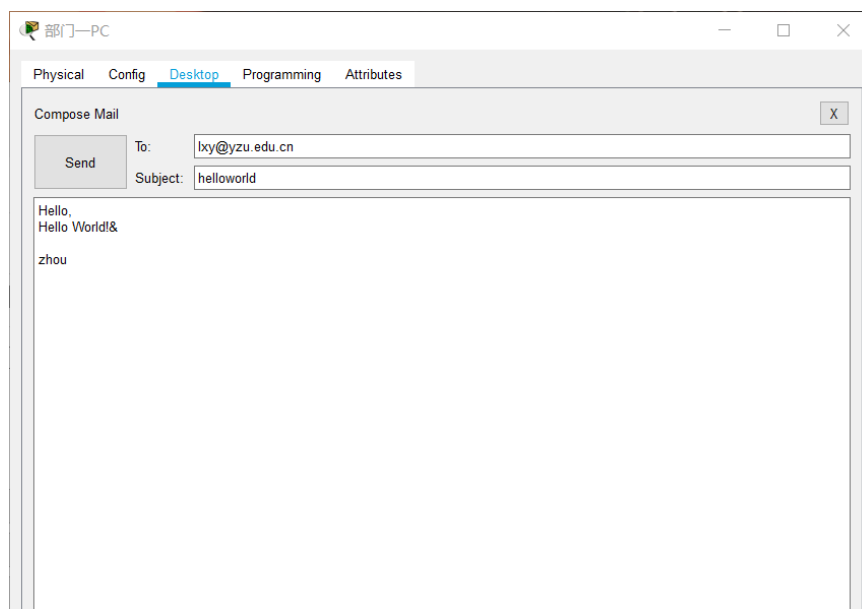


图 5.23 使用 mail 进行发送邮件

发送完成后，在该截图下方显示发送成功(最左下角)

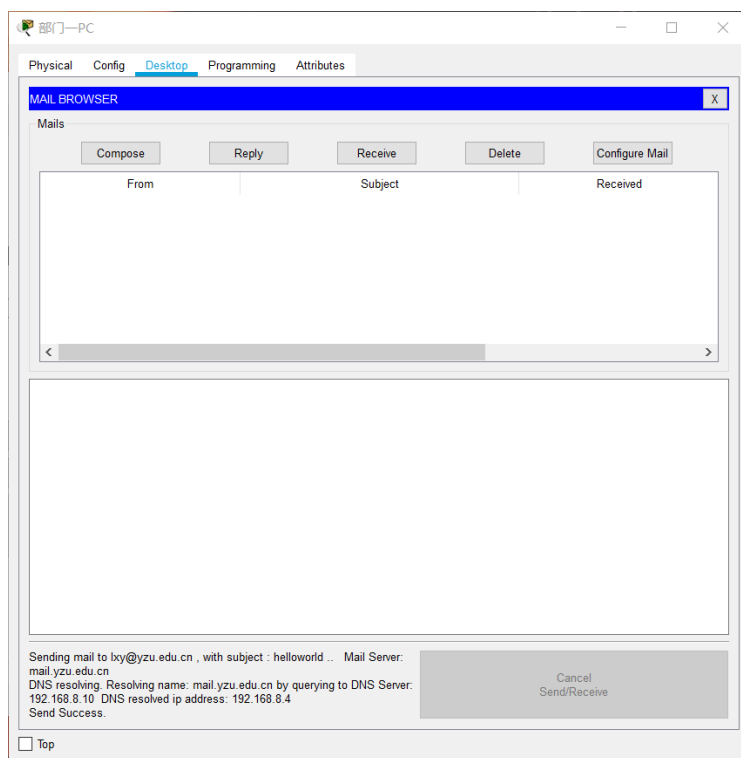


图 5.24 mail 发送邮件成功

可以看到 00:41:30 时刻从 <zhouzhou@yzu.edu.cn> 发来一封内容为“HELLOWORLD”的邮件

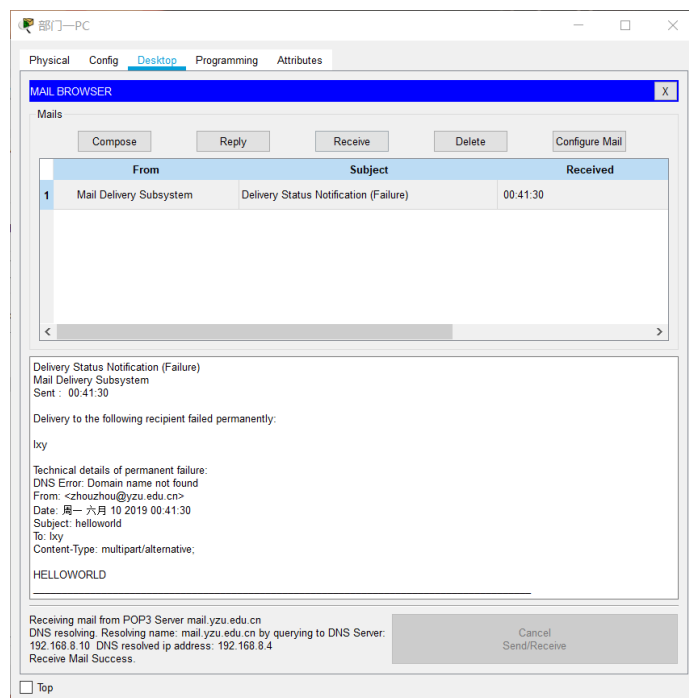


图 5.25 mail 接收邮件

5.4.5 DHCP 的测试

在 VLAN10 的三台不同主机上进行 DHCP IP 的 request 发现都成功 request 到了在 VLAN10 地址范围内的合法 IP

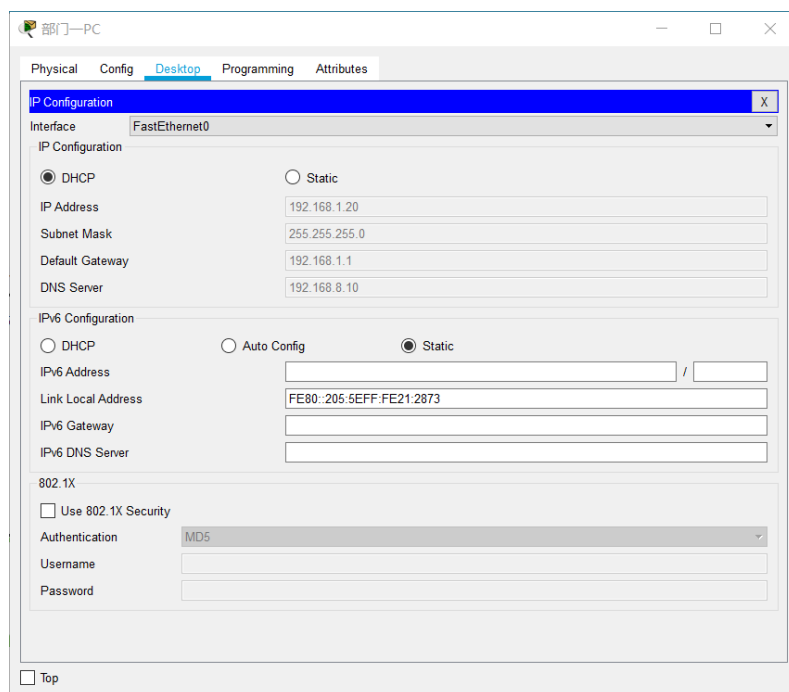


图 5.26 DHCP 分配部门一 PC

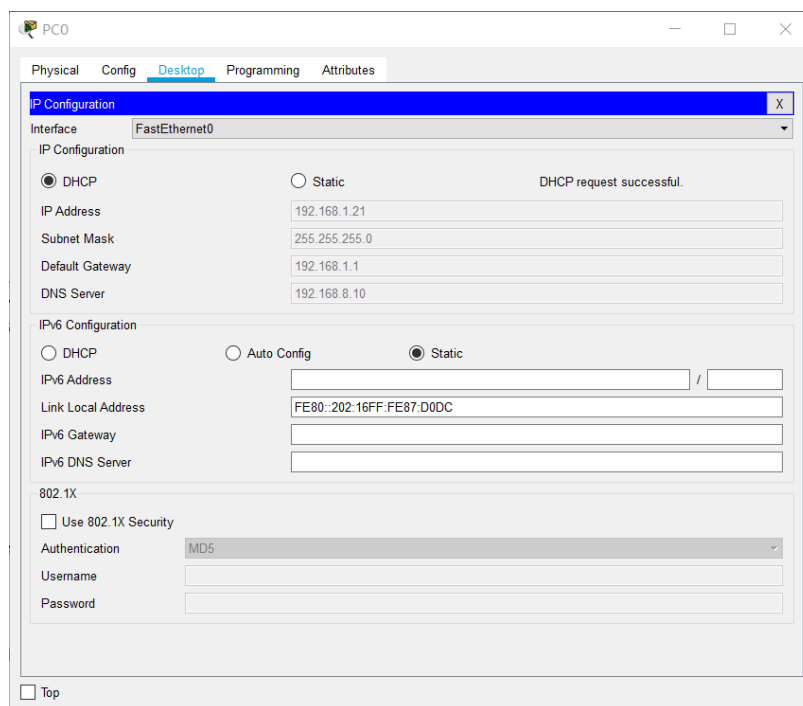


图 5.27 DHCP 分配 PC0

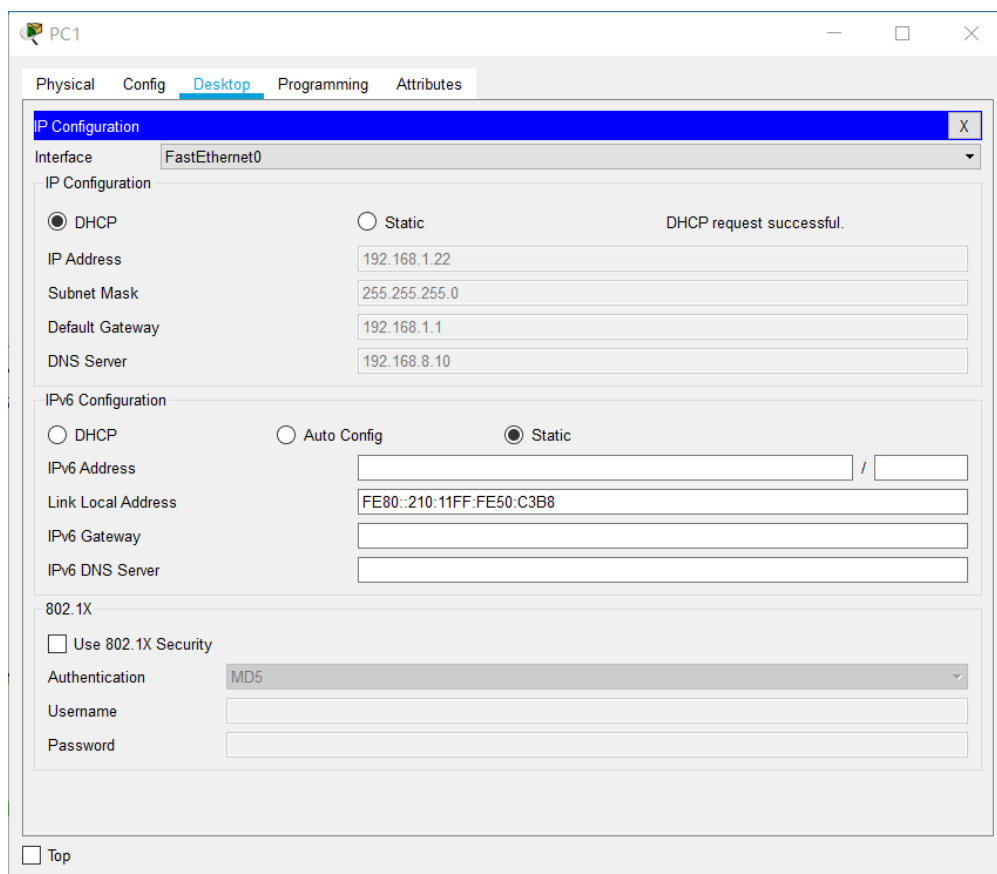


图 5.28 DHCP 分配 PC1

5.4.6 NAT 测试

外部 PC 不能访问内部 PC，出现了 Destination host unreachable。

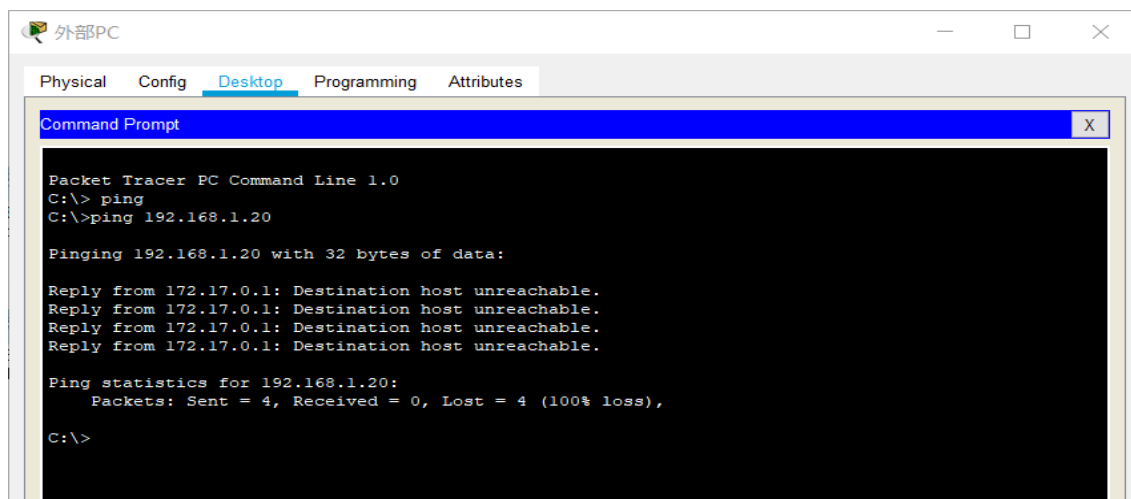


图 5.29 外部 PC ping 内部 PC

外部 PC 无法访问内部 OA 系统

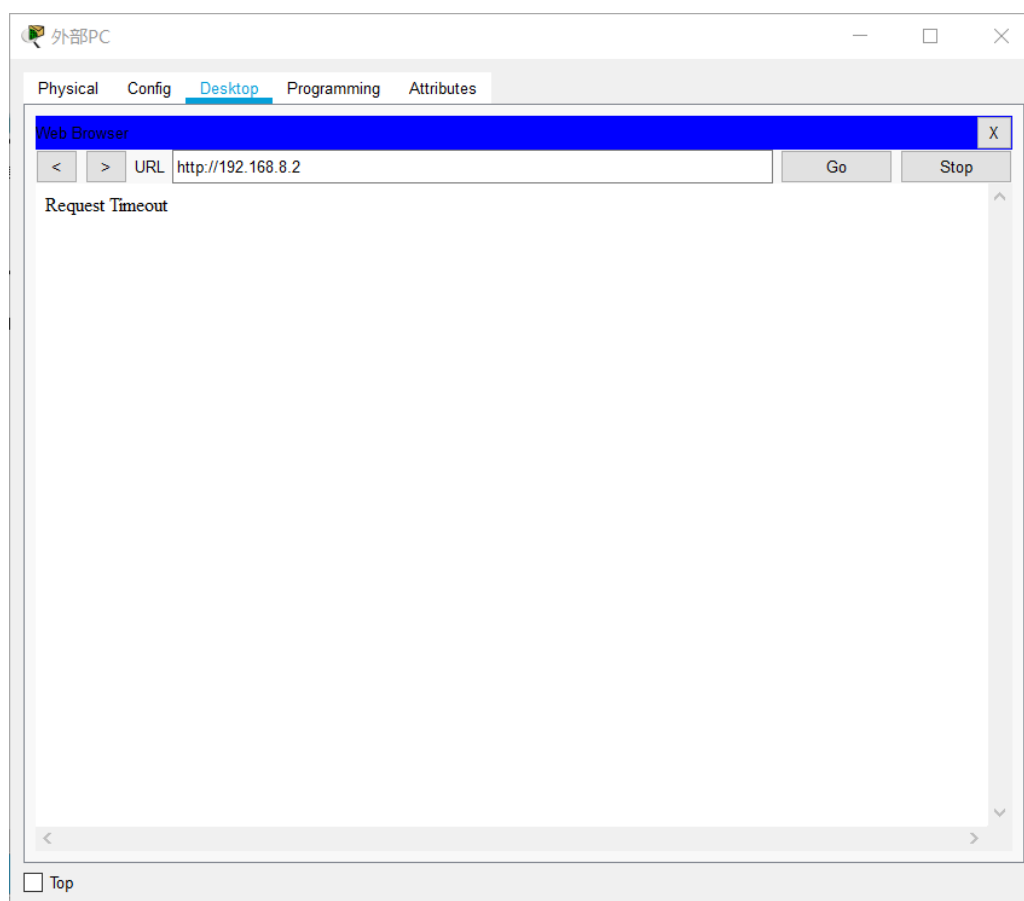


图 5.30 外部 PC 访问内部 OA

5.5 测试及分析中的注意事项

1.尽可能的穷尽所有情况进行测试，对于一些特殊的情况，要进行单独测试，比如对于不同的终端设备都要进行测试，对于 VPN 连接的情况也要进行有关的测试。

2.对于功能性测试要从不同角度反复进行测试，对于失败的测试，及时分析失败的原因，可能是由于刚刚启动，路由表中由于使用 rip 协议还没有该表项，所以需要较长时间才能测试成功。

第 6 章 网络其他设计

随着网络安全问题日益突出,网络的安全性和可靠性是构建网络系统时必须重点考虑的问题。本章着重于安全性设计和可靠性设计两方面,安全性设计采用的是 NAT+ACL 方式,详细分析了设计的具体过程和 NAT+ACL 的作用,过滤非法访问,可靠性设计 VRRP 技术,详细分析了 VRRP 技术的原理。

6.1 安全性设计

对于企业的业务局域网,威胁网络安全的主要因素是非法访问^[5]。经过充分调研,认真分析,结合企业的实际情况,我们采用 NAT+ACL 的方式对非法访问进行过滤。

ACL,即访问控制列表,其采用包过滤技术,通过预定义好的规则对包进行过滤,从而达到访问控制的目的。

设置 access-list 的具体规则的语句格式为:

```
access-list access-list-number [permit | deny ][sourceaddress] [wildcard-mask]
```

access-list-number 为 1-99 或者 1300-1999 之间的数字,即访问列表号。

在我们设置的 access-list 中,对内部的每个 VLAN 内的所有 PC 访问外网进行了全部放通,值得注意的是,即使是允许也必须在 ACL 中进行设置,因为 ACL 默认存在最后一条语句 deny any any,会对所有不符合规则的包全部进行丢弃

```
access-list 101 permit ip 192.168.0.0 0.0.0.255 any
```

```
access-list 102 permit ip host 192.168.1.0 0.0.0.255
```

```
access-list 102 permit ip host 192.168.2.0 0.0.0.255
```

```
access-list 102 permit ip host 192.168.3.0 0.0.0.255
```

```
access-list 102 permit ip host 192.168.4.0 0.0.0.255
```

```
access-list 102 permit ip host 192.168.5.0 0.0.0.255
```

```
access-list 102 permit ip host 192.168.6.0 0.0.0.255
```

在访问列表中,屏蔽以 172.17.0.0 (外网)的一整个网段访问 ftp 与内网 OA 的权限。

```
access-list 103 deny tcp any host 172.17.0.0 0.0.0.0 eq ftp www
```

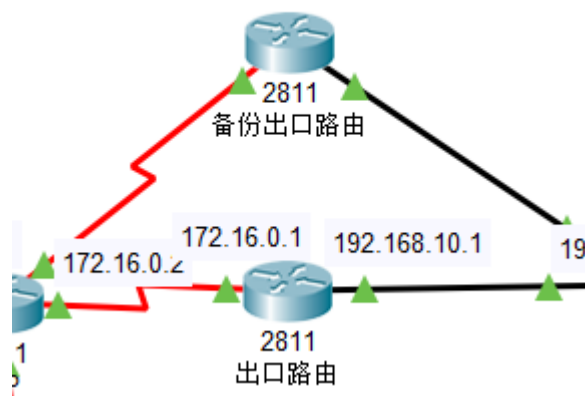
随后，在路由器出入口端口中应用 ACL 即可达到访问控制的目的，通过 `show access-lists` 可查看已经配置生效的 acl 信息。

ACL 是一种很灵活的访问控制方式，可以实现大部分访问控制需求，甚至还可以实现在不同时间段的访问控制。

同时，基于 ACL 的访问控制还提供了随时修改的可能，如果将来需要对内网的某台主机进行外网的访问限制，同样也可以在 `access-list 102` 中进行限制。因此，该网络的安全性设计具有高度的可拓展性。

6.2 可靠性设计

在系统最关键的节点之一——路由器处，我们设置了另一台路由器作为热备份，这里主要使用了 VRRP^[4] 技术，即虚拟路由器冗余协议。



如上图所示，我们选举主用服务器为“出口路由”，备用服务器为“备份出口路由”。即设置“出口路由”路由器状态为 Master，“备份出口路由”状态为 Backup。

当路由器处于 Master 状态时 它将会做下列工作：

- (1) 定期发送 VRRP 组播报文。
- (2) 发送免费的 ARP 报文，以使网络内各主机知道虚拟 IP 地址所对应的虚拟 MAC 地址。
- (3) 响应对虚拟 IP 地址的 ARP 请求，并且响应的是虚拟 MAC 地址，而不是接口真实 MAC 地址。

(4) 转发目的 MAC 地址为虚拟 MAC 地址的 IP 报文。

(5) 如果它是这个虚拟 IP 地址的拥有者，则接收目的 IP 地址为这个虚拟 IP 地址的 IP 报文，否则，丢弃这个 IP 报文。

在 Master 状态中只有接收到比自己的优先级大的 VRRP 报文时，才会转为 Backup。

当路由器处于 Backup 状态时，它会做下列工作：

(1) 接收 Master 发送的 VRRP 组播报文，从中了解 Master 的状态。

(2) 对虚拟 IP 地址的 ARP 请求，不做响应。

(3) 丢弃目的 MAC 地址为虚拟 MAC 地址的 IP 报文。

(4) 丢弃目的 IP 地址为虚拟 IP 地址的 IP 报文。

只有当 Backup 接收到 MASTER_DOWN 这个定时器到时的事件时，才会转为 Master。而当接收到比自己的优先级小的 VRRP 报文时，它只是做丢弃处理。

当主用链路出现故障时，主用路由的优先级被降权，“备份出口路由”被选举为主用路由，由于备份路由器处于开机状态，无需重新开机并加载配置文件，链路的切换耗时也比较短。对公司业务几乎不会造成影响。

核心代码：

```
(switch-config) interface fa0/7
(switch-config) ip address 192.168.10.1 255.255.255.0
(switch-config) no shutdown
(switch-config) interface fa0/3
(switch-config) ip address 192.168.8.1 255.255.255.0
(switch-config) no shutdown
(switch-config) ip address 192.168.8.1 255.255.255.0
(switch-config) vrrp vrid 1 virtual-ip 192.168.10.1
(switch-config) vrrp vrid 1 priority 50
(switch-config) vrrp vrid 2 virtual-ip 192.168.8.1
(switch-config) vrrp vrid 2 priority 100
```

同时，该网络结构的硬件设备均选用 Cisco 公司成熟设备，具有高度可靠性。

第7章 总结与体会

在本次课程设计的过程中，使用了 Cisco Packet Tracer 软件，完整实现了一个中小型企业网络规划与设计的方案，并较为系统地进行了各项测试。在实践过程中，大家感受到这是一次难度较大的课程设计，需要 Cisco Packet Tracer 软件基本操作的自学，包括软件配置，即使指令配置路由器，交换机等，硬件配置，包括串口等的配置等需要查找许多相关文档和视频材料。在撰写文档的过程中，发现写好一份文档和做好一份实验几乎同样困难，开始写文档的时候只是简单的截图的堆叠，之后开始逐步做好本次课程设计的整体细节，包括每一个配置的步骤，原因，最后进一步整理思路。在书写课程设计报告时，体会到了对于报告文档中的思路的重要意义和价值，如何通过一份文档使得实验结果得到准备，充分完备的展示。

纵观我们完成课程设计的整个历程，主要可以分为三个阶段：

第一阶段——“摸索与尝试”，最初拿到这个软件时，大家并没有感觉它和其他模拟仿真软件有什么不一样的地方。但是当我们初步摸索以后，我们才发现这个软件的优秀之处，首先，这个软件十分完美地模拟了路由器，交换机，PC 的基本功能，我们试着编写了几个基础脚本并部署，都得到了期望的效果。其次，该软件的优化十分不错，即使是打开一个 word 也也会占据很大的内存，cpu，可是当打开 Cisco Packet tracer 时，几十台 PC 同时运行同时发送消息都流畅的运作。

第二阶段——“学习与思考”，在尝试过 Cisco Packet Tracer 的各项基本功能之后，我们组再次组织讨论研习了本学期最后两个与 Cisco Packet Tracer 平台相关的课程实验，第一个和获取 TCP/IP 报文有关，在第一个实验中，我们了解了如何使用 Cisco Packet Tracer 进行慢速模拟和抓包，在第二个实验中，我们构建了一个星型网络，并且成功在每个主机上 ping 通了其余所有主机，此外，我们了解了如何连接交换机与交换机，交换机与 PC，线材的选取，交换机型号的选取，端口的选取等等。之后我们开始研读课程设计的相关要求，发现在其中的很多知识我们并不了解，如何在路由器上划分 Vlan，端口的 access 和

trunk 模式分别是什么，dhcp 地址池到底如何划分。对于 VPN 与 tunnel 的有关搭建开始也是完全没有头绪，通过反复查找相关资料，学习有关的视频，阅读思科教程。

第三阶段——“项目设计”，在以往的课程设计实验中，我们也体会到，从开始的一些零碎的知识到最终的课程设计之间还有着无数的障碍需要突破，在本次课设中也是一样。在实现和解决问题的过程中，我们对各项调试命令，比如 `tracert`, `ipconfig`, `ping`, `netstat` 等有了十分熟练的掌握。在给端口分配 `vlan`，路由器硬软件配置，`access-list` 设置方面，我们遇到了一些小困难，但得益于我们对基础知识都有过详细了解，即使中途有所卡住，也在反复思索排查问题之后得以解决。最后半天，我们对所有应用层的服务进行了实现，出乎我们预料的是，这一块是整个课程设计中最简单的部分，几种服务都只需要对服务器进行简单设置即可实现，同时，这也是最有成就感的时刻，当看到一封邮件从一个账户发送至另一个账户，PC 机成功读取 `ftp` 服务器上的内容，访问到公司内部 OA 和网站的时候，是非常有成就感的时刻。

在这次课程设计中，我们深刻体会到了具体的理论知识在实践中的运用，体会到了自己实践做出一个最终完整的系统的困难性，具体地，如何在网络上快速查找到自己需要的资料，如何通过这些资料快速研读，从中总结经验，对于遇到的困难，如何一步一步的排查，最终定位到错误的地方，解决这样的困难，在写文档方面，也是收获颇丰，文档的写作不仅仅是说明书，应当是整体构思的展现，简单的测试截图需要良好的阐释和说明才能成为一份合乎逻辑的测试。

最后，衷心感谢老师一学期以来给予的关心和指导，同学们的互相帮助！

参考文献

- [1] 褚健立.计算机网络技术[M].清华大学出版社.2006.9.
- [2] 谢希仁.计算机网络教程[M].人民邮电出版社.2002.5.
- [3] 吴功宜.计算机网络（第四版）[M].清华大学出版社.2017.4.
- [4] 韩明.试析 VRRP 协议在企业网络中的应用[J],2018,391(1):132-134.
- [5] 刘永华.计算机网络信息安全[M].北京:清华大学出版社.2014.
- [6] 吴功宜,吴英等编著.计算机网络课程设计[M].机械工业出版社.2012.
- [7] 莱特,斯蒂文斯著,路雪莹等译.TCP/IP 详解（卷 2）:实现[M].机械工业出版社.2004.
- [8] Cisco Packet Tracer 模拟器教程.下载网址:
https://www.cisco.com/c/m/zh_cn/offers/
- [9] 杨志姝. Cisco 实用教程（第三版）[M].北京:清华大学出版社.2005.
- [10] Anderson, Peter & Airi, Picky. Cisco Packet Tracer as a teaching and learning tool for computer networks in DWU[D].2017.
- [11] Honni, Honni & Andry, Johanes. Design and Simulation VLAN Using Cisco Packet Tracer: A Case Study[D].2016
- [12] 俞民华.三层交换机实现 VLAN 间互通的方法[J].福建电脑,2020,36(01):48-49.
- [13] 杨姝,罗佳.基于 Packet Tracer 软件的小型局域网络设计与仿真[J].实验技术与管理,2015,32(01):150-152.
- [14] 邱文军.NAT 技术及其虚拟网络实验教学研究[J].高教学刊,2016(14):103-104.
- [15] 高金丽.基于 Cisco Packet Tracer 的 DHCP 实验教学设计与实现[J].安徽电子信息职业技术学院学报,2015,14(03):42-46.