**山东大学（威海）**

**“数据通信与计算机网络”大作业**

|  |  |
| --- | --- |
| **学 院：** | **机电与信息工程学院** |
| **专 业：** | **电子信息工程** |
| **学 号：** | **202100800378** |
| **姓 名：** | **冯浩然** |
| **成 绩：** |  |

2024年1月2日

目录

[一 校园网综合设计 1](#_Toc154912548)

[（一）设计内容及设计目标 1](#_Toc154912549)

[（二）系统原理介绍 2](#_Toc154912550)

[1.编址规则 2](#_Toc154912551)

[2. 路由协议 2](#_Toc154912552)

[3. 内部网关协议 2](#_Toc154912553)

[4. 网络地址转换（PAT）技术 3](#_Toc154912554)

[5. 虚拟专用网络（VPN） 3](#_Toc154912555)

[6. 虚拟局域网（VLAN） 3](#_Toc154912556)

[7. 访问控制列表（ACL） 3](#_Toc154912557)

[8. 内网服务器端口映射 3](#_Toc154912558)

[（三） 系统设计及方案论证 4](#_Toc154912559)

[1. 系统设计： 4](#_Toc154912560)

[2. 方案论证 7](#_Toc154912561)

[（四） 系统性能仿真测试及分析 8](#_Toc154912562)

[1. 网络内部连通性测试 8](#_Toc154912563)

[2. 外网1与外网2连通性测试 10](#_Toc154912564)

[3. 济南内网与威海内网连通性测试 11](#_Toc154912565)

[4. 内网通过PAT访问外网测试 11](#_Toc154912566)

[5. 外网访问内网测试 12](#_Toc154912567)

[6. ACL测试 13](#_Toc154912568)

[7. VLAN测试 14](#_Toc154912569)

[8. DNS配置 15](#_Toc154912570)

[9. WWW网址访问测试 16](#_Toc154912571)

[10. 邮件测试 17](#_Toc154912572)

[11. 内部服务器端口映射测试 18](#_Toc154912573)

[（五）总结与体会 18](#_Toc154912574)

[二 论述题 19](#_Toc154912575)

[（一） 当前计算机网络面临的安全问题及解决措施。 19](#_Toc154912576)

[1. 安全问题 19](#_Toc154912577)

[2. 解决措施 20](#_Toc154912578)

[（二） 无线局域网关键技术分析。 24](#_Toc154912579)

[1. IEEEE 802.11 24](#_Toc154912580)

[2. 物理层关键技术 25](#_Toc154912581)

[3. 数据链路层媒体接入控制协议及关键技术 25](#_Toc154912582)

[4. 网络层路由协议及关键技术 26](#_Toc154912583)

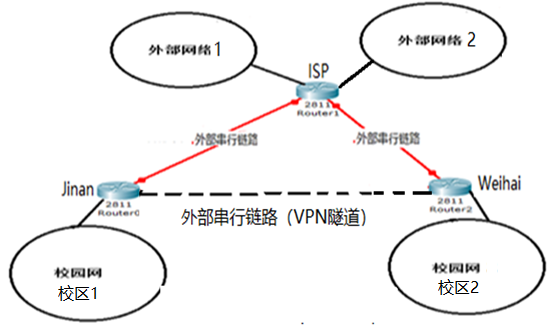
[5. 无线局域网应用 27](#_Toc154912584)

[参考文献 27](#_Toc154912585)

# 一 校园网综合设计

## （一）设计内容及设计目标

按照下图所示的结构，面向实际应用需求设计校园网，并对网络进行综合配置与仿真测试。该网络应满足以下要求：



**图1 校园网综合网络**

（1）校园网及外部网络应具有一定的规模，各网络的内部结构（子网数、各子网用户数）可以结合实际需求自行确定。

（2）采用无类别编址方式进行子网划分和IP地址分配，地址块可自行设定。校园网采用内部地址；外部网络采用外部地址，地址块根据需求由多个C类地址聚合而成；串行链路使用外部地址。

（3）外部网络采用动态路由协议，内部网络可采用静态路由和动态路由协议。

（4）校园网内用户采用地址转换访问外部网络，外部网络用户采用easy VPN访问内部网络。

（5）采用隧道技术实现校园网1与校园网2之间通过VPN进行通信。

（6）附加功能：VLAN、ACL、DNS、WWW、邮件服务、内网服务器端口映射、DHCP、无线接入等。

## （二）系统原理介绍

### 1.编址规则

#### （1）分类编址

分类编址是一种将IP地址空间划分为A、B、C、D和E五种类型的方法，每种类型有固定的地址范围，分别适用于不同规模的网络。A类适合大规模网络，B类适合中等规模网络，C类适用于小规模网络，D类专用于多播服务，而E类则保留未用。尽管分类编制直观易懂，但它导致了大量的地址空间浪费。  
 A类地址由32位二进制数组成，以0开头，第一个八位字节（即第一个字节）为网络部分，其余为主机部分，网络范围从1.0.0.0到126.0.0.0，1.0.0.0是保留地址，127.0.0.0用作回环地址。  
 B类地址以10开头，前两个字节为网络地址，后两字节为主机地址，网络范围是128.0.0.0至191.255.0.0。  
 C类地址以110开头，前三字节为网络地址，最后一个字节为主机地址，网络范围是192.0.0.0至223.255.255.0。  
 D类地址以1110开头，专用于多播，范围是224.0.0.0至239.255.255.255。  
 E类地址以1111开头，保留未用，范围是240.0.0.0至255.255.255.255。

#### （2）无分类编址

无分类编址方法通过使用更细小的子网划分来优化和灵活地使用IP地址空间，每个子网可以根据需要分配适当数量的地址。这种方法使用变长子网掩码（VLSM）来标识子网大小，极大提高了地址空间的利用效率。

### 2. 路由协议

#### （1）动态路由协议

动态路由协议通过自动配置，利用特定算法计算最优路径以实现数据包的有效传输。这类协议使得路由器能够与其他路由器交换信息并根据网络的变化自动调整路由表。它们主要应用于大型动态变化的网络环境中。典型的动态路由协议包括RIP和OSPF等，其中本实验将采用RIP协议。

#### （2）静态路由协议

静态路由协议依赖于网络管理员手动设置固定的路由路径，这些路径不会根据网络状况自动更新。它适用于小型或稳定网络，或在特定情况下需要确保路由路径不变的场合。静态路由的设置包括默认路由和特定路由等。

### 3. 内部网关协议

#### （1）PPP协议

PPP协议是一种常用于建立点对点连接的标准，广泛应用于拨号连接、DSL连接等场景，以建立两个节点之间的直接通信。

### 4. 网络地址转换（PAT）技术

#### （1）PAT技术

PAT，作为NAT技术的一种，不仅能将私有IP地址转化为公共IP地址，还能将相关联的私有端口号映射到公共端口号。这一技术支持多设备共享单一公共IP地址，并有效管理网络流量和资源。PAT广泛应用于大型企业网络环境中。

### 5. 虚拟专用网络（VPN）

#### （1）Easy VPN

Easy VPN通过IPSec协议提供加密和身份验证，确保连接安全。它支持远程访问和站点到站点连接，适用于需要远程安全连接的场景。

#### （2）隧道VPN

隧道VPN通过点对点连接将多个网络连接起来，通过互联网安全地传输数据。它可以采用IPSec、SSL、PPTP等多种协议加密，适用于高安全性的远程连接和多站点连接。

### 6. 虚拟局域网（VLAN）

#### （1）VLAN技术

VLAN技术通过逻辑分割，将一个物理网络划分为多个独立的逻辑网络。每个VLAN都有自己的网络地址、安全策略和流量管理，实现了不同虚拟网络间的隔离和优化通信。VLAN的实现主要依赖于交换机端口的配置。

### 7. 访问控制列表（ACL）

#### （1）标准ACL

标准ACL通过源IP地址过滤网络流量，提供基本的访问控制功能。

#### （2）拓展ACL

拓展ACL提供更细致的控制，能根据源IP地址、目的IP地址、协议类型、端口号等多种条件进行流量过滤和管理。

### 8. 内网服务器端口映射

#### （1）端口映射技术

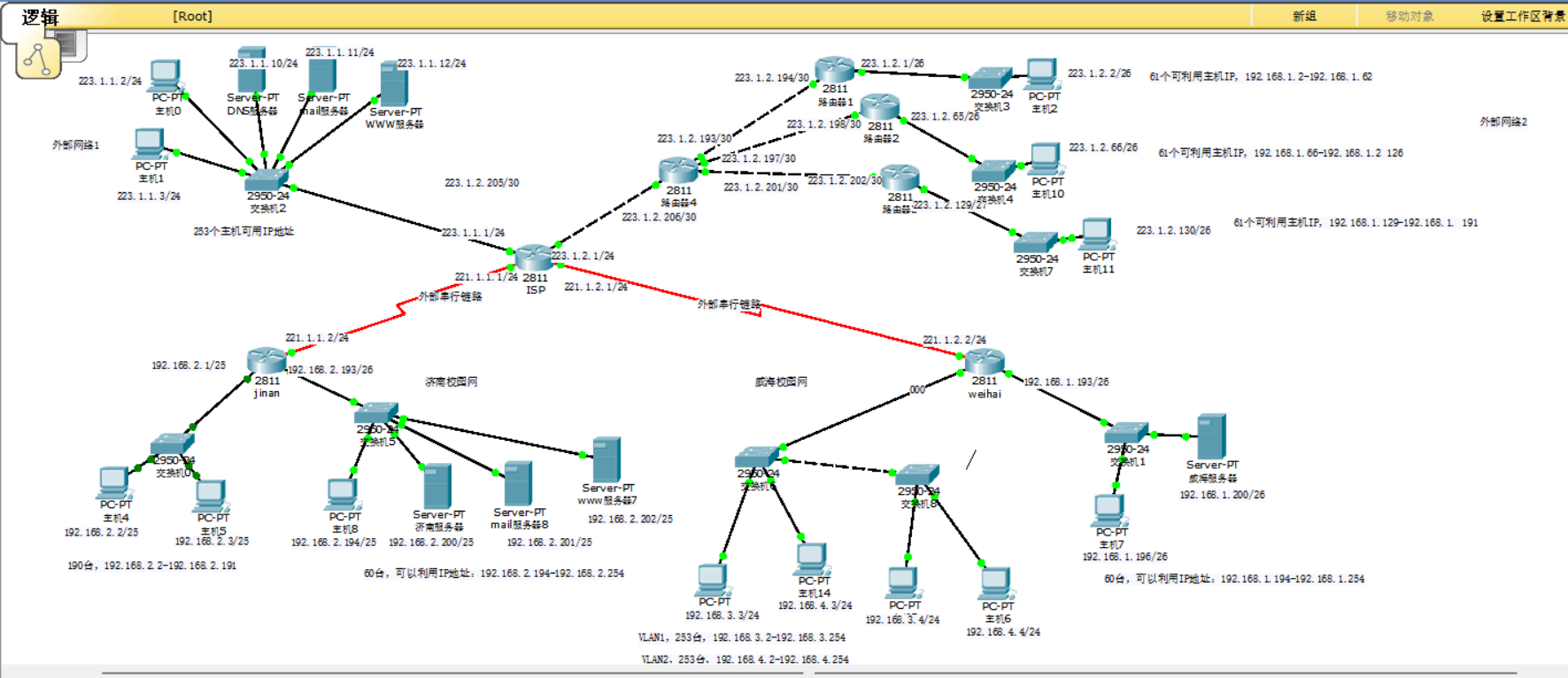
端口映射技术允许内部网络中的服务器通过公网IP地址被访问，实现远程连接和资源共享。本实验将采用端口映射技术，将公网IP地址的特定端口映射到内网服务器的端口，从而使外部用户能够通过特定的公网IP地址和端口号访问内网资源。

## 系统设计及方案论证

### 系统设计：

#### 整体拓扑结构

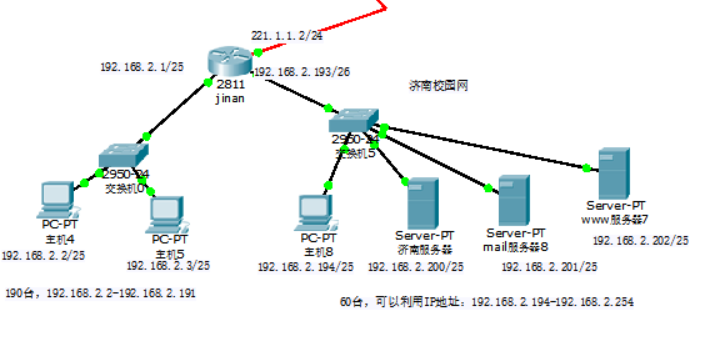
整个网络拓扑结构被划分为内部网络和外部网络。内部网络由济南校区和威海校区的校园网构成，每个校区都配备有专属的内部路由器，确保校内网络的稳定运行和管理。外部网络则分为外部网络1和外部网络2两部分。外部网络1直接连接至路由器ISP，形成一个直连网络，而外部网络2则包含多个路由器，具有更多的跳数，因此网络结构更为复杂。为了实现这些不同网络间的有效通信和数据传输，需要在外部网络1、外部网络2以及路由器ISP之间配置恰当的路由协议。这样的配置不仅确保了数据的顺利传递，还优化了网络路径，提高了通信效率



**图2 整体拓扑结构**

#### 济南校区校园网

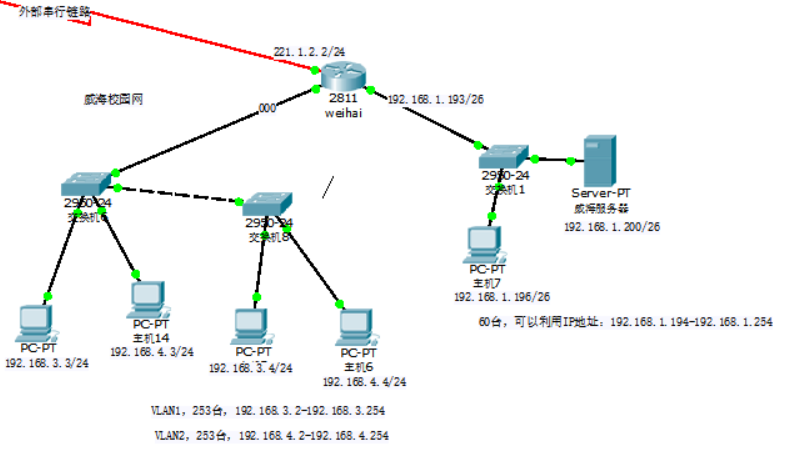
济南校区的校园网构成了路由器jinan的直连网络，涵盖了两个子网。此外，为确保校园网络及学工系统的顺畅运行，校区特别设置了DNS服务器、邮件服务器和WWW服务器。这些服务器不仅支持师生访问网站和学工系统，还能使他们发送和接收以xx@mail.sdu.com为地址的电子邮件，保障了通讯的便捷性和有效性。具体到子网划分，两个子网的地址分别是192.168.2.0/25和192.168.2.192/26，这样的划分有助于网络的组织和管理，确保网络资源的高效使用和安全。



**图3 济南校区校园网结构**

#### 威海校园网

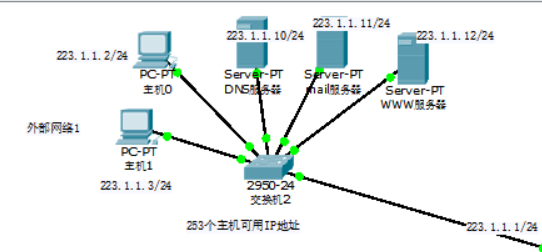
威海校区的校园网络构成了路由器威海的直连网络，它包括了一个主要子网及两个虚拟局域网（VLAN）。为了确保校区网络和学工系统的稳定性和可靠性，校区内还特别设立了DNS服务器。这种配置保障了威海校区网络的高效运行和师生的顺畅访问。具体到网络布局，子网地址为192.168.3.0，而两个VLAN的地址分别配置为vlan1: 192.168.4.0和vlan2: 192.168.1.192/26。这样的网络架构不仅优化了资源分配，还强化了网络的管理和安全控制。



**图4 威海校区校园网结构**

#### 外部网络1

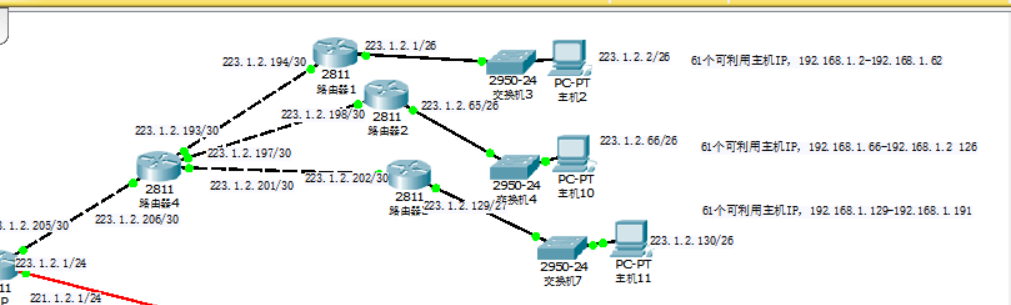
外部网络1是路由器ISP的直连网，设有外部的DNS服务器、mail服务器和WWW服务器。子网号为223.1.1.0。



**图5 外部网络1结构**

#### 外部网络2

外部网络2构成了一个覆盖三个部门的复杂网络结构，这个网络通过路由器ISP进行连接，但需两跳才能完成访问，其中并没有设立独立的服务器。在这个网络中，路由器ISP与路由器4，以及路由器4与路由器1、路由器2和路由器3之间的连接，都位于各自独立的子网中。这些子网的地址分别为223.1.2.204/30、223.1.2.192/30、223.1.2.196/30和223.1.2.200/30。与此同时，三个部门的子网号分别设为223.1.2.0/26、223.1.2.64/26和223.1.2.128/26。这样的网络布局确保了不同部门之间的通信独立性和网络的整体运作效率。



**图6 外部网络2结构**

#### 路由器ISP

路由器ISP构成了网络的核心节点，它分别与外部网络1、路由器4、路由器jinan和路由器weihai建立了连接。特别地，与路由器weihai和路由器jinan的连接是通过外部串行链路实现的，这些链路的子网号分别为221.1.1.0/24和221.1.2.0/24。为了确保这些连接的稳定性和安全性，路由器ISP与路由器jinan和路由器weihai之间都需要配置PPP协议、PAT协议和Easy VPN协议。这样的配置不仅提升了数据传输的效率和安全性，也保证了网络在不同环境下的适应性和可靠性。

#### （7）路由器jinan

路由器jinan中，配置了ACL协议，允许威海校区访问济南校区内网。

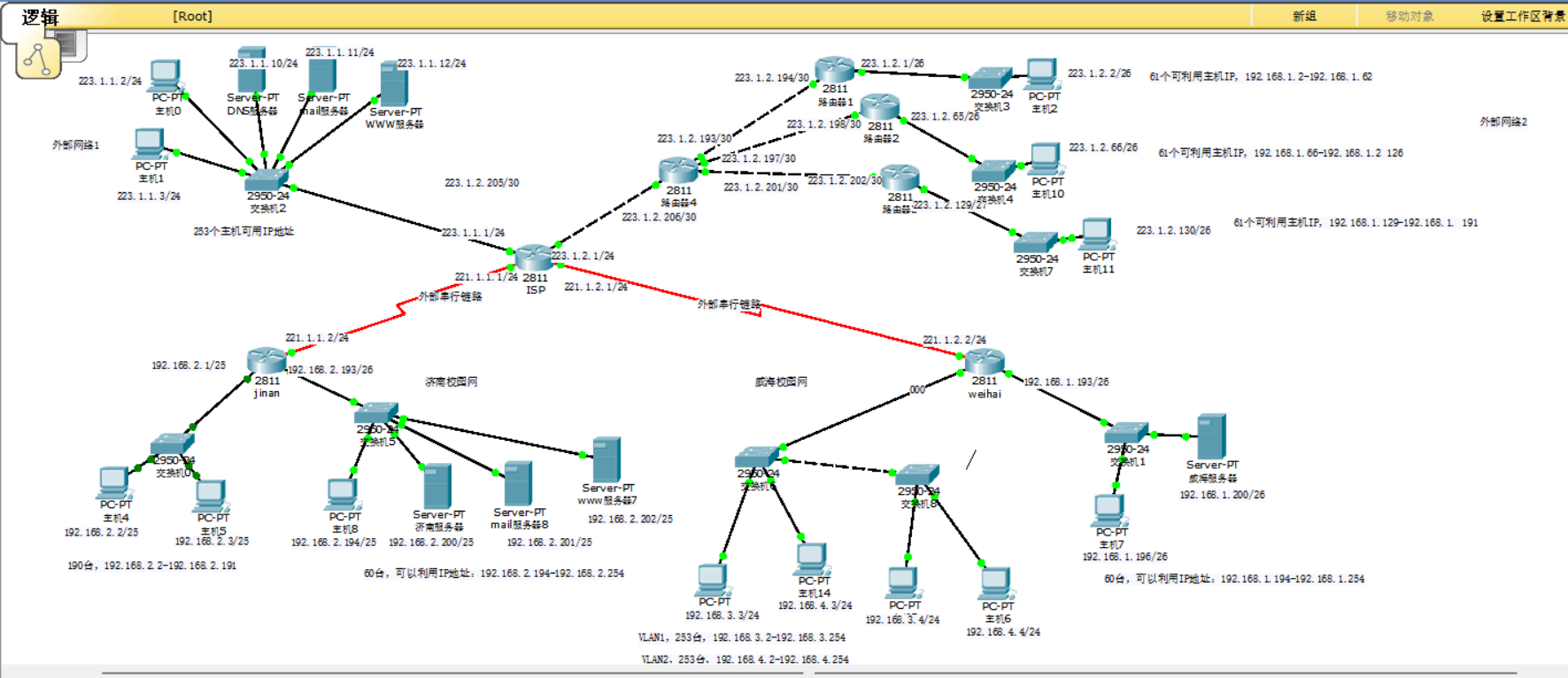
#### （8）路由器weihia

路由器weihai中，给网络划分了VLAN。

### 方案论证

#### （1）拓扑结构

左上角为外部网络1，右上角为外部网络2，左下角为济南校区内网，右下角为威海校区内网。



**图7 网络拓扑结构**

#### （2）网络划分

外部网络1：子网号为223.1.1.0/24，253个可以用主机IP地址。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| LAN1 | 子网地址 | 子网掩码 | 网关 | PC0主机号 | 可使用ip范围 |
| 223.1.2.0 | 255.255.255.192 | 223.1.2.1 | 223.1.2.2 | 223.1.2.2-223.1.2.62 |
| LAN2 | 子网地址 | 子网掩码 | 网关 | PC1主机号 | 可使用ip范围 |
| 223.1.2.64 | 255.255.255.192 | 223.1.2.65 | 223.1.2.66 | 223.1.2.66-223.1.2.126 |
| LAN3 | 子网地址 | 子网掩码 | 网关 | PC0主机号 | 可使用ip范围 |
| 223.1.2.128 | 255.255.255.192 | 223.1.2.129 | 192.168.1.130 | 223.1.2.129-223.1.2.191 |
| LAN4 | 子网地址 | 子网掩码 | 网关 | 下一跳路由节点IP | 可使用ip范围 |
| 223.1.2.192 | 255.255.255.252 | 223.1.2.193 | 223.1.2.194 | 223.1.2.193-223.1.2.194 |
| LAN5 | 子网地址 | 子网掩码 | 网关 | 下一跳路由节点IP | 可使用ip范围 |
| 223.1.2.196 | 255.255.255.252 | 223.1.2.197 | 223.1.2.198 | 223.1.2.197-223.1.2.198 |
| LAN6 | 子网地址 | 子网掩码 | 网关 | 下一跳路由节点IP | 可使用ip范围 |
| 223.1.2.200 | 255.255.255.252 | 223.1.2.201 | 223.1.2.202 | 223.1.2.201-223.1.2.202 |
| LAN7 | 子网地址 | 子网掩码 | 网关 | 下一跳路由节点IP | 可使用ip范围 |
| 223.1.2.204 | 255.255.255.252 | 223.1.2.205 | 223.1.2.206 | 223.1.2.205-223.1.2.206 |

**表1 外部网络2网络划分**

外部网络2：

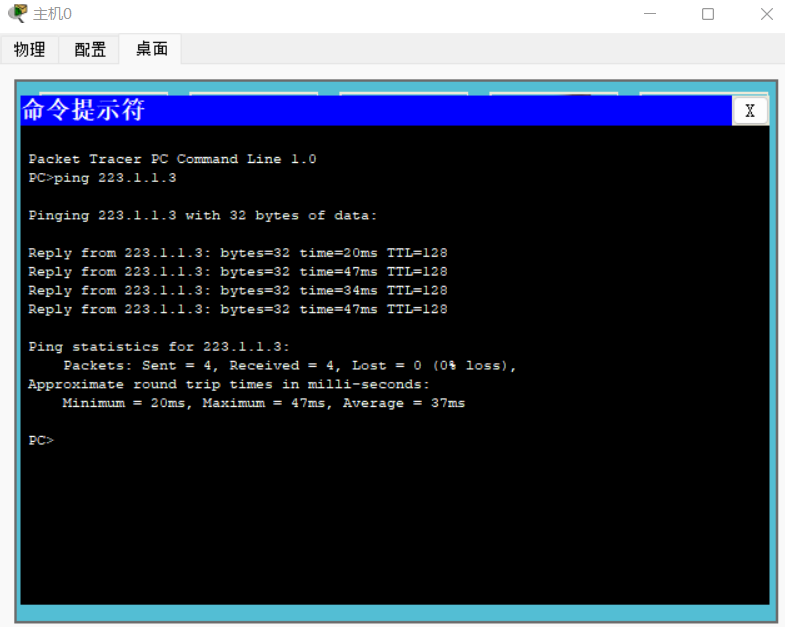
济南校园网：两个子网号分别为192.168.2.0/25和192.168.2.192/26。分别容纳190台主机和60台主机。

威海校园网：子网号分别为和vlan1：192.168.3.0、vlan2：192.168.4.0和192.168.1.192/26。分别容纳253、253、60台主机。

## 系统性能仿真测试及分析

### 网络内部连通性测试

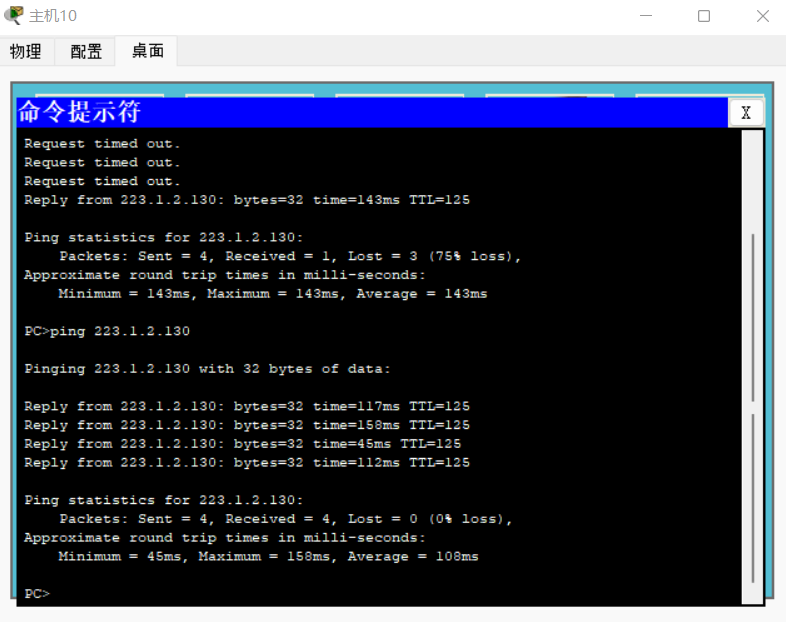
#### 外部网络1的内部联通



**图8 主机0访问主机1**

由此说明，外网1内部可以连通。

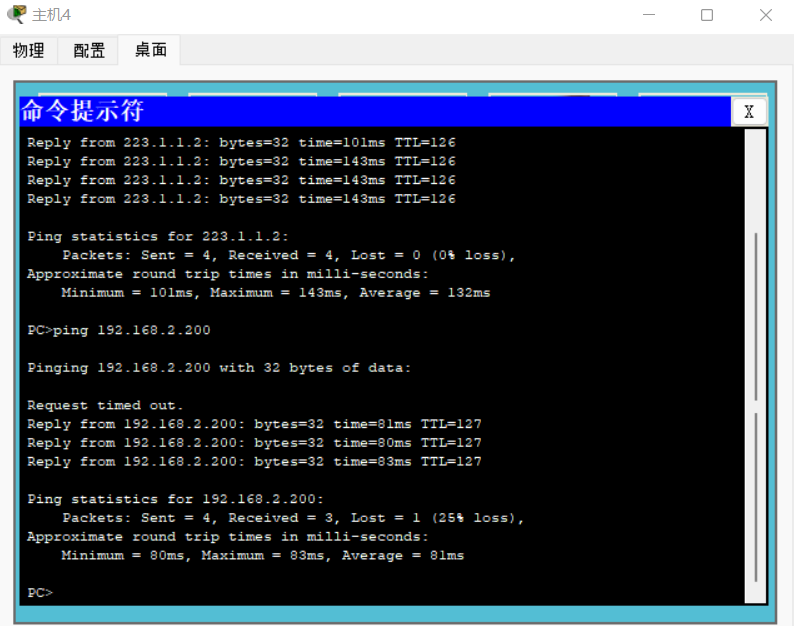
#### 外部网络2的内部联通



**图9 主机10访问主机11**

由此说明，外网2内部可以连通。

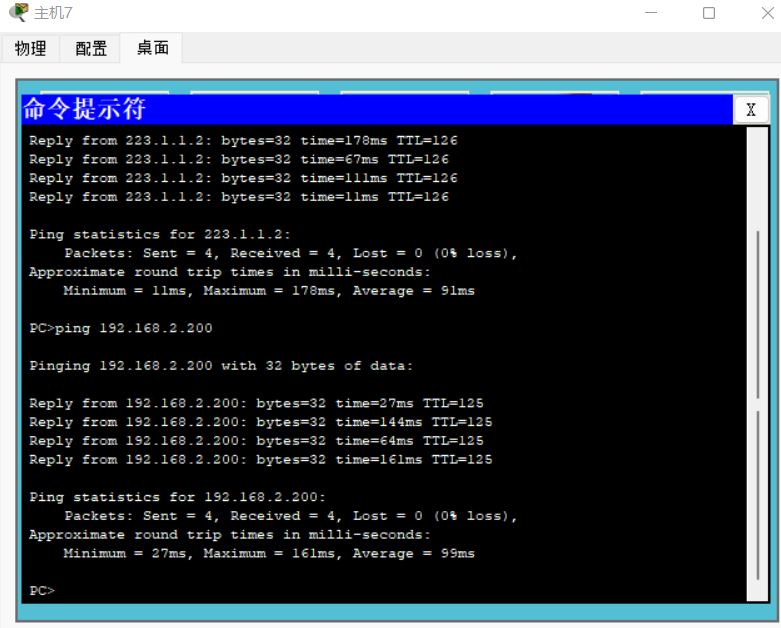
#### 济南校区校园网的内部联通



**图10 主机4访问济南校区服务器**

由此说明，济南校园网内部可以连通。

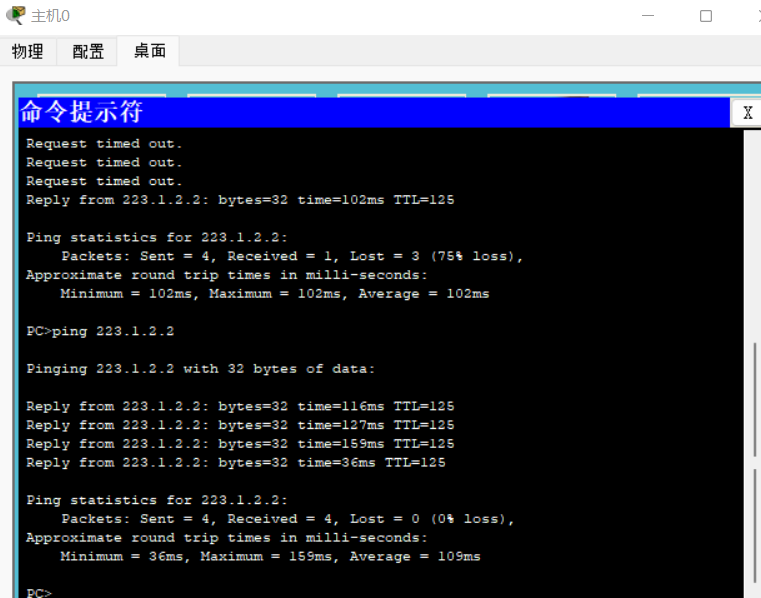
#### 威海校区校园网的内部联通



**图11 主机7访问威海校区服务器**

由此说明，威海校园网内部可以连通。

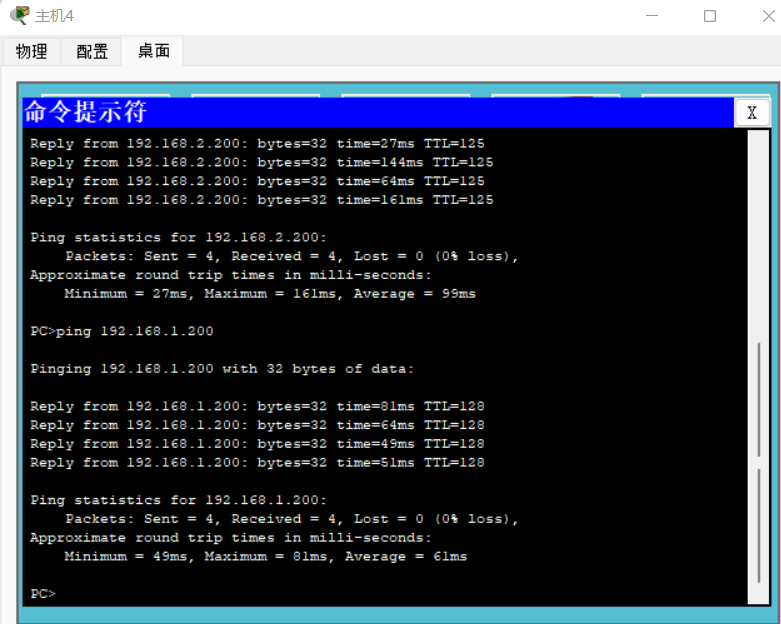
### 外网1与外网2连通性测试



**图12 主机0访问主机2**

由此说明，外网1和外网2可以连通。

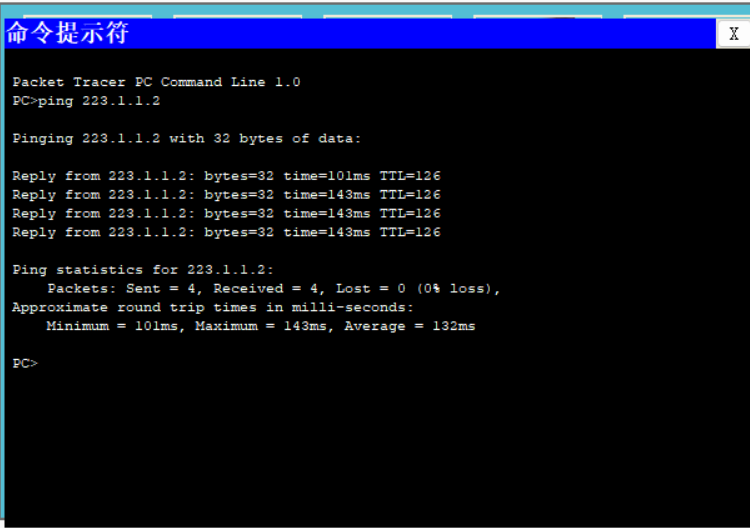
### 济南内网与威海内网连通性测试



**图13 主机4访问威海校区服务器**

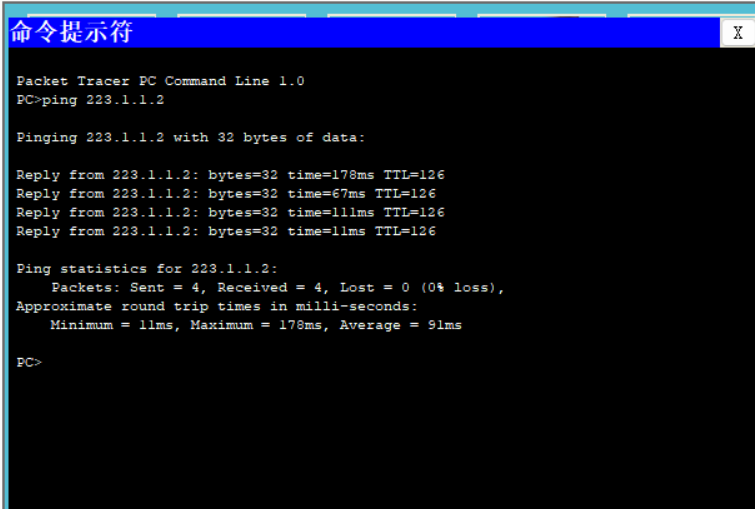
由此说明，济南校园网和威海校园网可以连通。

### 内网通过PAT访问外网测试



**图14 主机4访问外网主机0**

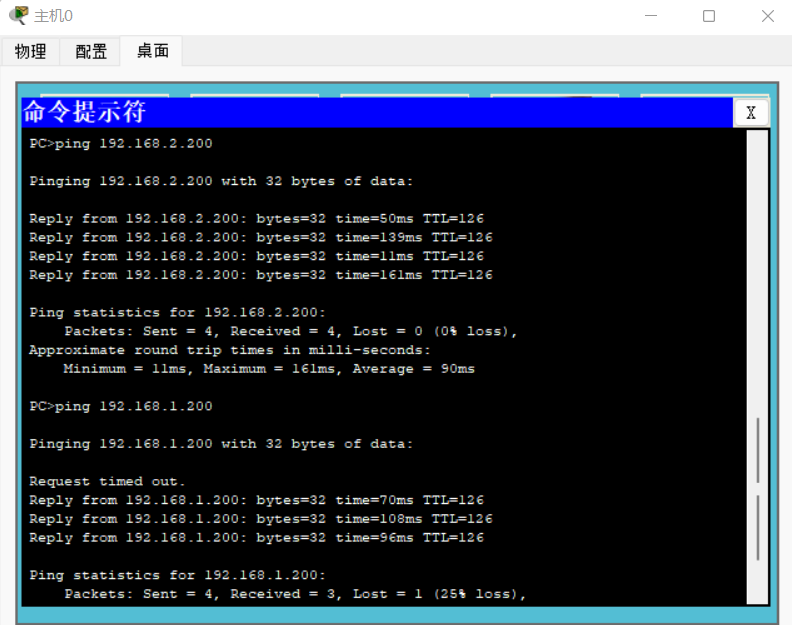
由此说明，济南校区可以访问外网。



**图15 主机7访问外网主机0**

由此说明，威海校区可以访问外网。

### 外网访问内网测试

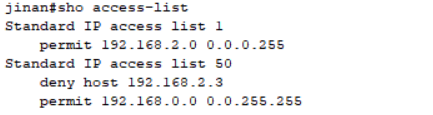


**图16 外网主机0访问济南和威海校园网的服务器**

由此说明，外网可以访问济南校园网和威海校园网。

### ACL测试

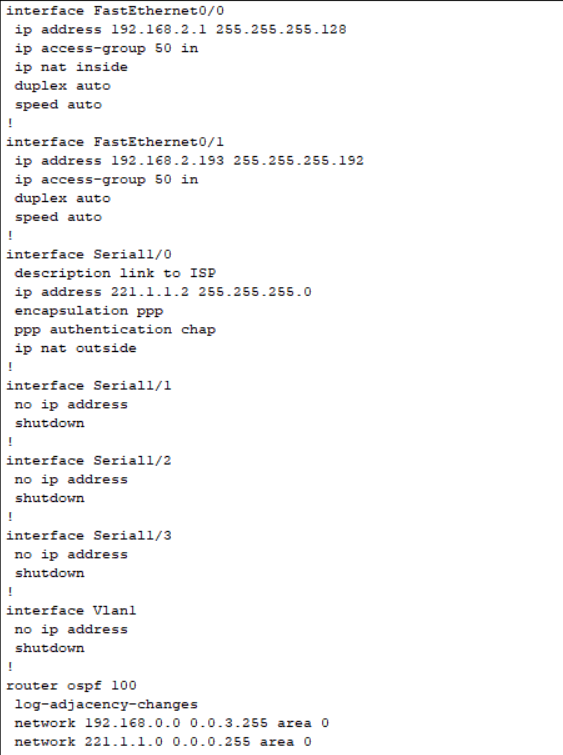
#### 济南校园网的路由器jinan查看访问控制列表



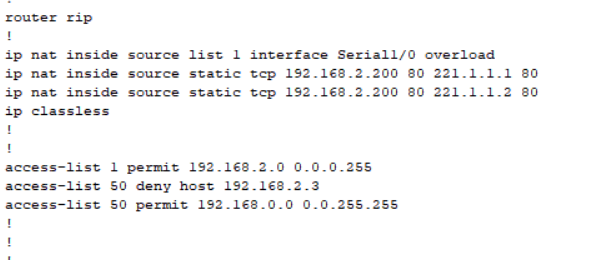
**图17 济南校园网的ACL**

由此可知，路由器jinan允许192.168.2.0/24的IP地址访问济南校园网，允许192.168.0.0/16的IP地址访问济南校园网，但是不允许主机号192.168.2.3的主机访问济南校园网。

#### 济南校园网的路由器jinna查看运行状态

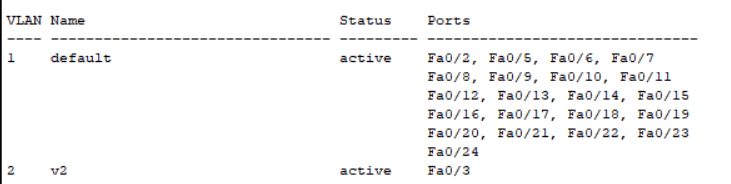


**图18 路由器jinan的运行状态**

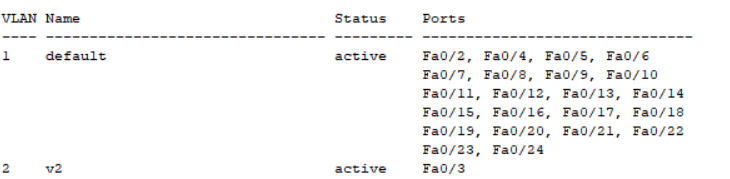


**图18（续） 路由器jinan的运行状态**

### VLAN测试



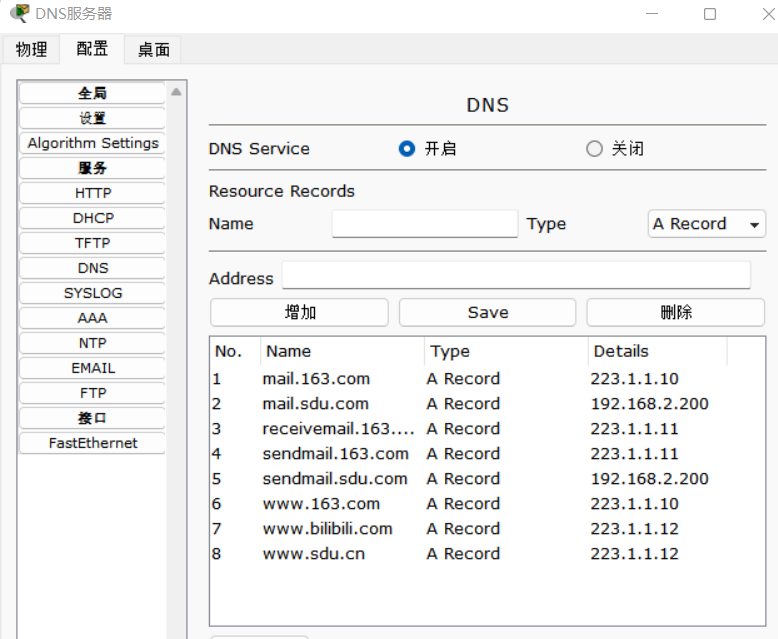
**图19 威海校园交换机6的VLAN**



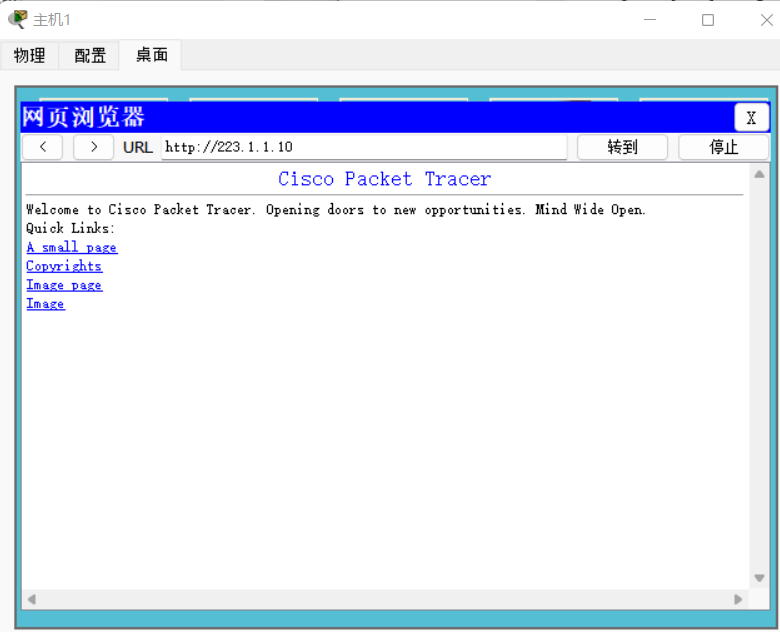
**图20 威海校园交换机8的VLAN**

由此可知，交换机6的端口2的主机9、交换机8的端口2的主机3属于VLAN1，交换机6的端口3的主机14、交换机8的端口3的主机6属于VLAN2，

### DNS配置



**图21 外部网络1的DNS服务器配置**



**图21 外部网络1主机1通过IP地址访问DNS服务器**



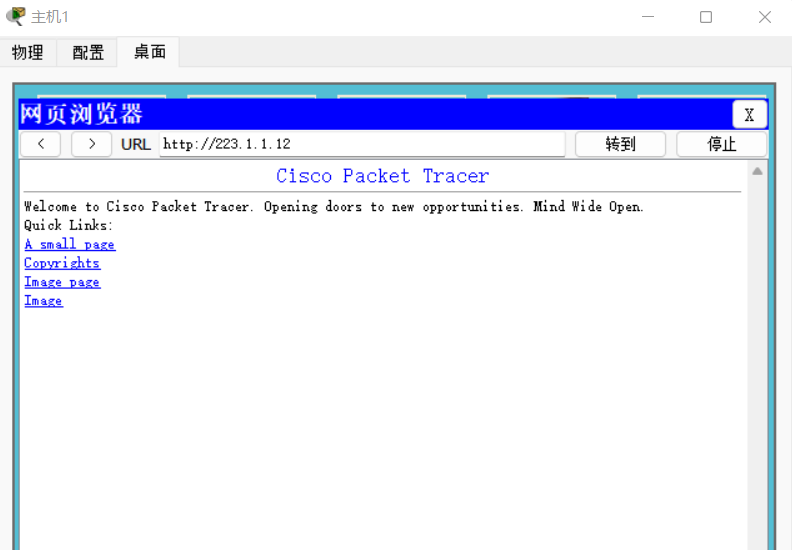
**图22 主机1通过网址访问mail.163.com**

由此可知，DNS服务器配置成功，主机可以通过访问DNS服务器的IP地址从而访问mail.163.com,也可以直接输入网址进行访问。

### WWW网址访问测试



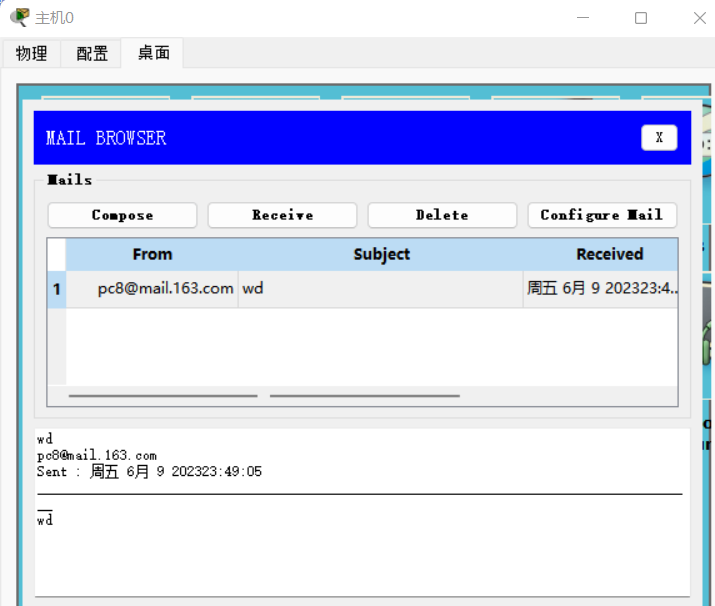
**图23 主机1访问www.sdu.cn**



**图24 主机1通过IP地址访问WWW网页**

由此可知，主机可以通过输入www网址来访问网页，也可以输入WWW服务器的IP地址223.1.1.12进行访问。

### 邮件测试



**图25 主机0和主机8之间的互通邮件**

由此可知，邮件功能可以正常使用。

### 内部服务器端口映射测试



**图26 济南校园网的路由器NAT**

将192.168.1.67的80端口与201.1.1.2的80端口进行映射，当从外网中的主机访问http://201.1.1.2时，指向内网192.168.1.67WWW服务器的主页。

## （五）总结与体会

这次的网络设计项目是一个对之前课程学习和七次实验知识的全面实践和应用。它不仅加深了我对计算机网络技术的理解，而且提升了我的网络设计和实施能力。通过实际操作，我得以将理论与实践紧密结合，对网络技术的多个方面有了更深刻的认识。

在设计过程中，我成功实现了内网和外网的互连，并实现了网络间的邮件交换和DNS查询。此外，我通过VLAN技术有效地进行了子网划分，大大减少了广播风暴的可能性。同时，在济南校区网络中引入ACL配置，实现了威海校区网络对济南校区网络的访问控制，并能够阻止特定主机的访问。

当然，设计过程中也面临了不少挑战。VPN的配置特别容易出现错误，导致主机VPN登录超时。隧道VPN的配置也需要多次尝试才能成功，确保济南和威海校区网络的互通。这些挑战强化了我的解决问题和调试的能力，让我更加明白在计算机网络领域，实践和持续学习的重要性。

通过本次设计，我深刻体会到理论知识和实际操作的重要性。在未来的学习和工作中，我将继续探索和实践，不断提升自己在计算机网络领域的专业水平和实践能力。

# 二 论述题

## 当前计算机网络面临的安全问题及解决措施。

### 安全问题

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 被动攻击 | 截获 | 攻击者在网络上窃听他人通信内容。攻击者在不干扰目标系统正常运行的情况下，仅仅是监听和截取目标系统的通信流量，以获取敏感信息。因不直接干预系统运行，被动攻击通常难以被发现。 | | |
| 主动攻击 | 篡改 | | 攻击者未经授权修改目标系统中的数据或程序，以达到恶意目的。篡改攻击会对目标系统造成实际的破坏或干扰，因攻击者需要修改数据或程序。 | |
| 恶意程序 | 计算机病毒 | | 一种恶意软件，通过复制自身并插入其他程序或文件中来感染计算机系统。病毒可以未经授权执行各种恶意操作，如删除文件、损坏数据或窃取个人信息。 |
| 计算机蠕虫 | | 与病毒不同，蠕虫能够自我复制并传播到其他计算机系统。它们利用网络漏洞感染计算机，可能导致网络拥塞或系统崩溃。 |
| 特洛伊木马 | | 看似有用但实际上是恶意的程序，隐藏在其他程序或文件中，在用户不知情的情况下执行恶意操作。通常用于窃取个人信息、监视用户活动或控制受感染的计算机。 |
| 逻辑炸弹 | | 设计为在特定条件下触发的恶意程序，如特定日期或时间、特定用户登录时或在特定操作执行后。触发后，逻辑炸弹可以删除文件、损坏数据或破坏系统。 |
| 后门入侵 | | 黑客通过利用系统漏洞或弱点获取未经授权的访问权限。利用后门，黑客可以窃取敏感信息、操纵系统或执行其他恶意操作。 |
| 主动攻击 | 恶意程序 | 流氓软件 | | 未经用户明确同意而安装的软件，通常会在用户不知情的情况下收集个人信息、弹出广告或执行其他恶意操作，通常伪装成有用的程序或附加在其他软件中。 |
| 拒绝服务攻击  （DoS攻击） | | | 旨在使目标计算机或网络资源无法提供正常服务的网络攻击。攻击者通过发送大量请求或数据流量使目标超负荷或崩溃。 |
| 新攻击类型 | AI驱动攻击 | | | 利用人工智能技术适应和学习防御措施的攻击，使得攻击更加复杂化、难以预测和对抗。 |
| 供应链攻击 | | | 通过攻击软件或硬件供应商来对最终目标或多个依赖被攻击组件的目标进行攻击的方式。 |

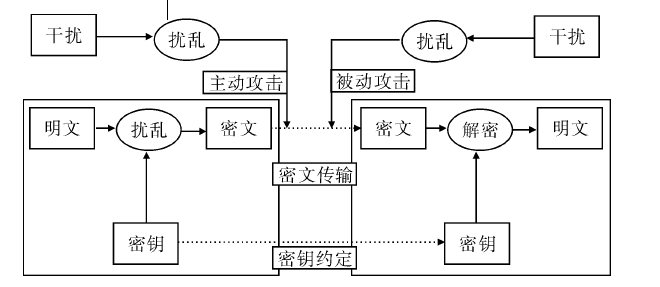
**表2 计算机网络面临的安全问题**

### 解决措施

#### （1）加密技术

针对被动（截获）攻击，需要各种加密技术，利用公钥密码体制可以有效地进行加密，防止攻击。

任何加密系统不论形式多么复杂都至少包括明文、密文、加解密装置或算法和密钥4部分组成。加密系统模型如图26所示。

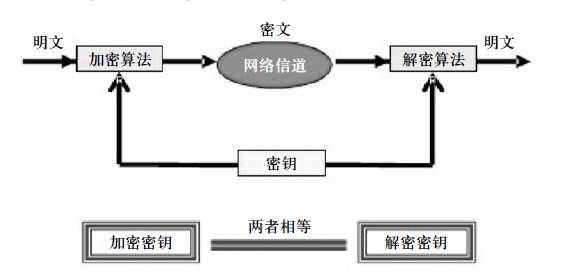


**图26 数据加密模型**

##### 对称加密

对称加密又叫做共享密钥加密，是指信息发送方和接收方使用相同的密钥

进行加密和解密数据，这要求通信双方在安全传输密文之前必须商定一个公用密钥。因此，只有密钥未被双方泄露的情况下，才能确保传输数据的安全性、机密性和完整性。[6]



**图27 对称密钥加密（保密密钥）示意图**

对称加密技术是最常用的数据加密技术，它的数据加密算法主要有DES、AES 和IDEA。DES 数据加密标准算法是一种对二元数据加密的算法，它是一个对称的64 位数据分组密码，密钥为任意56 位，剩余8 位为奇偶校验。DES 加密速度快、效率高，其加密范围广泛，成功应用于银行电子资金转账领域。

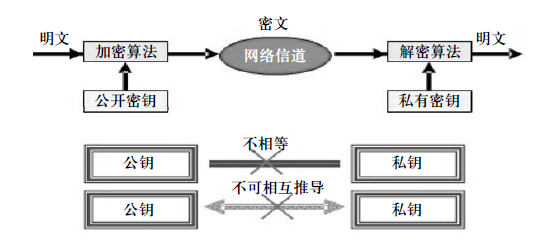
##### 联邦数据加密标准（DES）算法

DES 算法的数据流程的基本框架是固定的通过密钥分解将一个实际上是56bit 的密钥分解为16个48bit 的子密钥每个子密钥控制一次迭代。加密与解密的密钥和程是完全相同的区别仅仅是加密与解密使用子密钥序的施加顺序刚好相反。DES 数据加密系统流程的主要步骤如下：[7]

1. 输入64bit 码的明文；
2. 初始置换IP移位操作；
3. 乘积变换这是一个与密钥有关的对码组加密运算；
4. 逆初始置换1／IP是第②步的逆变换；
5. 输出64bit 密文

##### 非对称加密技术。

非对称加密又叫做公钥加密，是指信息发送方和接收方使用不同的密钥进行加密和解密数据，密钥被分解为公开密钥（加密）和私有密钥（解密），现有的技术和设备均未能由公钥推出私钥。非对称加密技术以密钥交换协议为基础，通信的双方无须事先交换密钥便可直接安全通信，消除了密钥安全隐患，提高了传输数据的保密性。[6]



**图28 非对称密钥加密（公开密钥）示意图**

非对称加密技术的数据加密算法主要有RSA、Diffie-Hellman、EIGamal、椭圆曲线等，典型的RSA 算法可以抵抗当前已知的所有密码攻击，它是应用最广泛的著名的公钥算法。非对称加密技术不仅仅适用于数据加密，还可以进行身份认证和数据完整性验证，广泛用于数字证书、数字签名等信息交换领域。

##### RSA 密码体制

RSA 算法是建立在具有大素数因子合数的因子分解是困难的基础上的即它的保密强度是建立在计算复杂性基础上的。一个150位左右的合数即使采用现在的巨型电子计算机进行因子分数其运算量也是相当巨大的。

下面将RSA 算法运作的步骤总结如下：

1. 随机地选择两个秘密的素数p 和q；
2. 计算公开的模数 (1)
3. 计算秘密的欧拉指示函数 (2)
4. 选择一个与互素的， 可以定义为秘密密钥或公开

密钥；

1. 将明文（其值在之间）自乘 次幂后按取模进行加密运算产生密文（其值在之间）；

(3)

1. 将密文（其值在之间）自乘 次幂后按取模进行解密运算产生明文（其值在之间）。

(4)

#### 防火墙

防范网络攻击最常用的方法是防火墙[8]。防火墙作为一种边界安全， 能较有效地保护网络内部的安全，并在保护网络安全中起到了重要作用。从技术理论讲， 防火墙属于最底层的网络层安全技术。但随着网络安全技术的发展， 现在， 防火墙已经成为一种更为先进和复杂的基于应用层的网关， 不仅能完成传统防火墙的过滤任务， 同时也能够针对各种网络应用提供相应的安全服务。利用防火墙技术， 经过仔细的配置，通常能够在内外网之间提供安全的网络保护， 降低网络安全的风险。

根据防范的方式和侧重点的不同， 防火墙大致可分为三大类􀀈

##### 数据包过滤

该技术是在网络层对数据包进行选择， 选择的依据是系统内设置的过滤逻辑，即访问控制表。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素， 以及它们的组合来确定是否允许该数据包通过。它通常安装在路由器上。

##### 牌用级网关

在网络的应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑， 并在过滤的同时对数据包进行必要的分析、登记和统计， 形成报告。应用网关通常安装在专用的工作站系统上。

##### 代理服务

也称链路级网关或TCP通道，它将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间的应用层的“ 链接”，由两个终止于代理服务器上的“ 连接” 来实现。外部计算机的网络链路只能到达代理服务器， 从而起到了隔离防火墙内外计算机系统的作用。此外， 代理服务器也对过往的数据包进行分析、注册登记，形成报告，同时当发现攻击迹象时会向网络管理员发出警报，并保留攻击痕迹。

#### 控制流量

控制流量是控制流量是网络管理的一个关键方面，专注于监测和调节通过网络的数据传输速率，以优化性能、避免拥塞和保护网络免受某些类型的攻击，如拒绝服务攻击（DoS）和分布式拒绝服务攻击（DDoS）。流量控制技术通常包括以下几个方面：

**速率限制：**定义网络或特定链接上允许通过的最大数据量。这有助于控制带宽使用，保持网络性能，并在高流量情况下防止服务下降。

**流量整形：**调整数据包的发送速率，延缓或重新安排数据包的传输，确保重要的数据优先传输，同时避免突发流量造成的网络拥塞。

**队列管理：**使用各种队列算法（如FIFO、RED、WRR）来管理数据包的处理和传输顺序，优化网络响应时间和带宽利用率。

**拥塞避免：**通过探测网络拥塞的早期迹象并适时调整传输速率来预防网络拥塞，保持网络的稳定运行。

**策略执行：**根据定义好的策略（如访问控制列表、服务质量规则等）来控制流量，允许或拒绝特定类型的流量，确保网络资源符合业务需求和安全政策。

通过这些控制流量的技术和策略，网络管理员可以有效地管理网络资源，保证网络服务的质量，同时减轻潜在的安全威胁。流量控制不仅有助于提升用户体验，还是实施网络安全策略的重要手段。

## 无线局域网关键技术分析。

### IEEEE 802.11

IEEE 802.11是一组用于局域网（LAN）无线通信的标准。IEEE 802.11标准定义了一种无线网络技术，它允许计算机、移动设备和其他设备通过无线信号进行通信和互联。

#### IEEEE 802.11工作原理

IEEE 802.11标准采用无线电波在设备间传递数据，并实现通信。为了有效管理数据传输，它运用了一种名为“载波感应多路访问/碰撞避免”（CSMA/CA）的技术。此协议要求设备在发送数据前检测信道是否空闲，确保同一时刻只有一个设备进行数据发送。如果信道忙碌，设备会暂停发送并在随后的时间里重新尝试。

在IEEE 802.11的操作流程中，客户端设备首先搜索周边的无线网络，寻找可连接的接入点（AP）。一旦锁定目标AP，客户端会发送连接请求并进行身份验证。验证通过后，客户端和AP之间的连接建立，随即开始数据传输。

在数据传输阶段，客户端将信息拆分为一系列小数据包进行发送。这些数据包被AP接收后重新组装，并通过有线网络传递到目标地址。反向传输时，AP也将来自有线网络的数据拆分成数据包，再发送至客户端设备。整个过程涵盖了从数据包的生成、发送到接收和重组，确保信息准确无误地在无线网络中传递。

#### （2）无线接入点AP

无线接入点（AP）通常配备了一或多根天线，负责发送和接收无线信号。作为连接无线通信和有线网络的桥梁，AP将通过有线方式与路由器、交换机或其它网络设备连接，并将有线信号转发为无线格式。根据IEEE 802.11标准，无线接入点充当网络中的核心节点，使得无线设备得以接入有线网络。用户的无线设备既可以通过AP与网络或其他设备沟通，也能实现点对点的直接通讯。

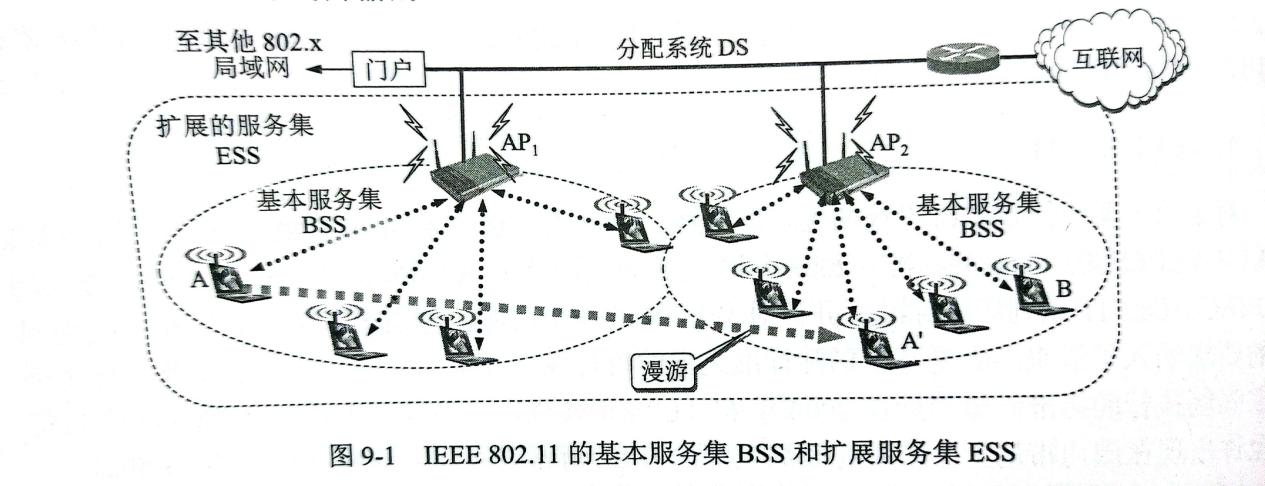
#### （3）IEEE 802.11服务集

①基本服务集（BSS）

基本服务集是由一个AP和多个无线客户端设备组成的一个小型网络。在BSS中，无线客户端设备通过AP连接到有线网络，从而实现无线和有线网络之间的通信。

②扩展服务集（ESS）

扩展服务集是由多个BSS组成的一个大型网络。在ESS中，多个AP通过有线网络连接起来，形成一个无缝的覆盖范围，使得无线客户端设备可以在不同的BSS之间自由切换，从而实现无缝的无线网络覆盖。



**图29 IEEE的基本服务集和拓展服务集**

#### （4）安全机制

IEEE 802.11标准制定了一系列安全措施，包括WEP、WPA和WPA2，旨在增强无线网络的安全性，抵御未经授权的访问和潜在攻击。这些安全机制的引入显著提升了网络防护能力。其中，WEP曾是初期的保护手段，但由于其较弱的加密方式，较易受到破解；而WPA和WPA2则分别代表了安全技术的进步，它们通过采用更为高级的加密技术和身份验证方法，为无线网络提供了更为坚实的防护屏障。

### 物理层关键技术

**802.11a：**工作在5 GHz频段，提供最高54 Mbps的传输速率。这一标准采用了OFDM技术，通过将数据均匀分布在多个子载波上，提升了传输的效率和稳定性。

**802.11b：**利用2.4 GHz频段，其传输速率上限为11 Mbps。这一技术使用DSSS技术进行数据传输，通过扩展信号在宽广频段上的占用，提高信号的鲁棒性。

**802.11g：**同样操作在2.4 GHz频段，并提供最高54 Mbps的速率。802.11g融合了OFDM技术，并保持对802.11b的兼容性，提供了速率与兼容性的平衡。

**802.11n：**支持2.4 GHz和5 GHz双频段，最高传输速率可达600 Mbps。它引入了MIMO技术，即多天线的发送和接收，显著提高了传输速率和覆盖范围。

IEEE 802.11协议族不止包括这些，还有如802.11ac、802.11ax等更先进的物理层技术。这些标准进一步细化和发展了无线传输技术，如FHSS、DSSS、OFDM等，各自有着独特的机制和优势，共同提高了无线网络传输的速度和可靠性。这些技术的发展，持续推动着无线网络技术朝着更高速度、更大容量和更广覆盖面的方向发展。

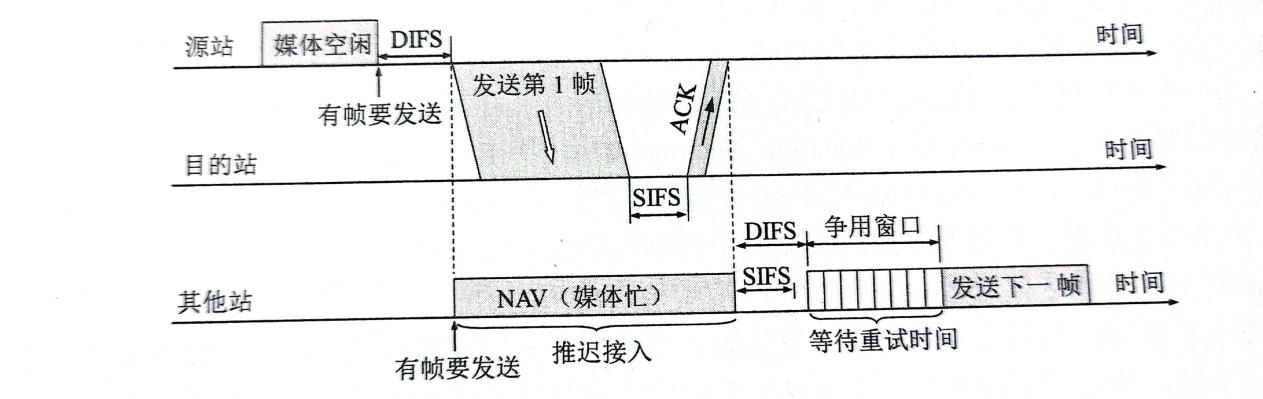
### 数据链路层媒体接入控制协议及关键技术

数据链路层媒体接入控制协议（MAC协议）是计算机网络中用于控制多个设备共享同一物理媒体的协议。它的主要作用是协调多个设备之间的通信，防止冲突和混乱。

常见的MAC协议及其关键技术：

#### CSMA/CA（载波侦听多路访问/碰撞避免）

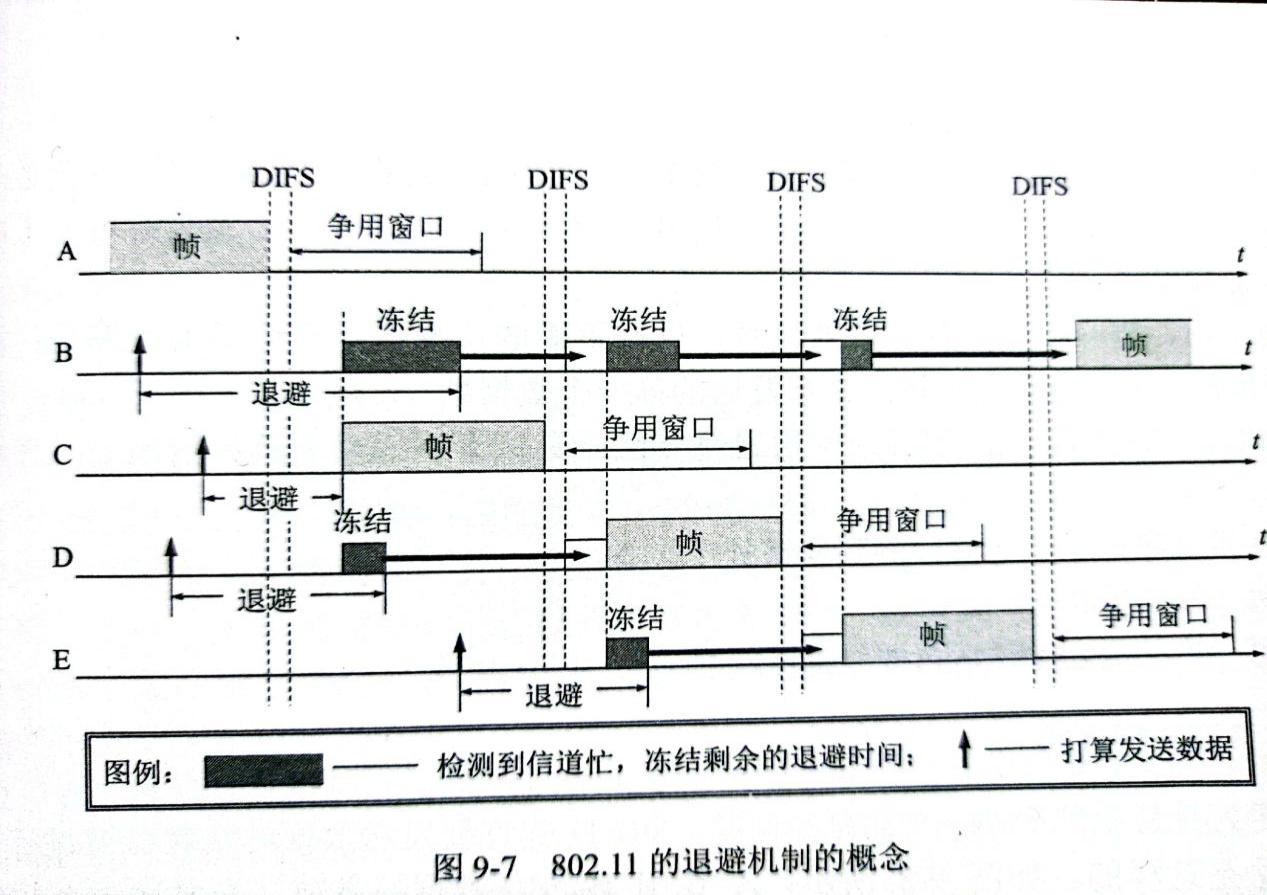
这种协议采用了与CSMA/CD相似的原理，但引入了碰撞避免技术以降低数据传输中的冲突概率。在CSMA/CA协议下，设备想要进行数据传输前会先发送一个RTS（请求发送）帧来告知网络中的其他设备其传输意图。收到这一请求的设备随后回复CTS（清除发送）帧，确认对RTS帧的接收。这种交互确保了网络中的设备都能了解到谁将占用信道，从而协调彼此的发送时机，有效避免了数据传输的冲突。



**图30 CSMA/CA协议的工作原理**

#### （2）IEEE802.11退避机制

在IEEE 802.11标准中，设备欲在无线信道上进行数据传输前，必须首先确认信道的空闲状态。若信道正被其他设备使用，该设备将进入等待状态，并周期性地重新检查信道。这一等待过程是通过一种称为退避机制的策略实现的。该机制规定，设备在探测到信道忙碌时，会随机决定一个等待时长，称为退避时间，完成后再次进行信道空闲检测。如果信道依旧不可用，设备将重复此退避过程，直至成功探测到可用信道。这种方法有效平衡了信道访问，减了冲突，保证了网络的稳定通讯。



**图31 802.11的退避机制**

### 网络层路由协议及关键技术

IEEE 802.11标准指定了无线局域网（WLAN）的物理层和数据链路层的通信协议。该标准构成了无线网络通信的核心框架，而非具体的路由协议。它确立了无线通信的基本规则和参数，为在无线网络环境中实现有效的数据传输提供了基础。在基于IEEE 802.11的网络中，可以根据具体需求和环境，灵活采用各种路由协议来优化和管理网络路由，从而增强网络的性能和可靠性。

### 无线局域网应用

无线局域网技术因其灵活性、便捷性和高效性而被广泛应用于多种场景，如家庭、企业和公共场所等。在家庭环境中，无线局域网主要用于连接各种设备，支持家庭成员之间的无线通信和娱乐活动；企业网络通过无线方式连接员工和资源，提升办公效率和灵活性；而公共场所如咖啡馆、图书馆和机场等，则通过提供无线上网服务，满足人们移动办公或休闲时的网络需求。无线局域网的推广和应用，极大地丰富了现代生活的网络体验，使得信息交流更为快捷，生活和工作更加高效和便利。

# 参考文献

1. 谢希仁. 计算机网络（第8版）[M]. 北京：电子工业出版社，2021：324-401
2. 刘刚. 无线局域网(WLAN)建设中的关键技术分析[C]. 2002’中国通信学会无线及移动通信委员会学术年会. [会议地城市不详], 2002: 550-553.
3. 冯宪光.无线局域网技术发展现状及未来趋势[J].计算机产品与流通,2019,2019(04):88.
4. 张利红.IEEE802.11n网络协议关键技术分析[J].齐齐哈尔大学学报(自然科学版),2014,30(05):42-46.
5. 唐高阳.数据加密技术在计算机网络安全中的实践探析[J].软件,2023,44(11):85-87.
6. 朱闻亚.数据加密技术在计算机网络安全中的应用价值研究[J].制造业自动化,2012,34(06):35-36.
7. 王秀翠.数据加密技术在计算机网络通信安全中的应用[J].软件导刊,2011,10(03):149-150.
8. 张然,钱德沛,过晓兵.防火墙与入侵检测技术[J].计算机应用研究,2001(01):4-7.