



北 京 科 技 大 学

# 《计算机网络》 设计型报告

专业班级：\_\_\_\_信安 211\_\_\_\_

姓 名：\_\_\_\_李晓坤\_\_\_\_

学 号：\_\_\_\_U202141863\_\_\_\_

成 绩：\_\_\_\_\_

2023 年 12 月 30 日

## 目 录

1.设计目的 .....	2
2.设计内容 .....	3
2.1 设计要求 .....	3
2.2 设计实现 .....	3
3.实现步骤 .....	5
3.1 拓扑图设计 .....	5
3.2 IP 规划表 .....	5
3.3 主要技术 .....	7
3.3.1 VLAN 间通信技术 .....	7
3.3.2 网络路由配置 .....	7
3.3.3 NAT 技术 .....	8
3.3.4 静态路由配置 .....	8
3.3.5 IPv4 与 IPv6 共存 .....	8
3.3.6 DHCP 技术 .....	9
3.3.7 DNS 技术 .....	9
3.3.8 FTP 技术 .....	9
3.4 设备配置 .....	10
3.4.1 DHCP 相关配置 .....	10
3.4.2 数据中心基本配置 .....	13
3.4.3 外网基本配置 .....	15
3.4.4 路由配置 .....	17
3.4.5 NAT 配置 .....	17
3.4.6 DNS 服务器配置 .....	18
3.4.7 FTP 服务器配置 .....	20
3.4.8 IPv6 实现 .....	20
3.5 测试验证 .....	23
3.5.1 基本连通测试 .....	23
3.5.2 DHCP 配置测试 .....	24
3.5.3 NAT 配置测试 .....	26
3.5.4 DNS 服务器配置测试 .....	27
3.5.5 FTP 服务器配置测试 .....	29
3.5.6 IPv6 配置测试 .....	30
二、总结与收获 .....	32
1.项目总结 .....	32
2.课程收获 .....	32

# 一、《基于思科模拟器的 IPv6 校园网》设计

## 1. 设计目的

选择大作业（一）：**基于思科模拟器的 IPv6 校园网设计**

整个实验分为两部分：第一部分建立基本的校园网，实现内网 PC 连通外网、外网 PC 访问内部的 WEB 服务器；第二部分在第一部分的基础上进行改动，增加系统设计的功能。在报告展示中，将这两个部分进行合并展示，详细内容见报告后续。

- （1）校园网设计：基于前 4 次实验学到的知识，进行 IPv6 校园网设计。
- （2）理解校园网络的基本要求：掌握校园网络设计的基本概念，包括网络拓扑、子网划分、网络设备的选择和部署。
- （3）熟悉思科模拟器的使用：学习使用思科模拟器进行网络设备的模拟和配置，包括路由器、交换机、终端设备等。
- （4）设计合理的 IP 地址方案：通过合理的 IP 地址规划，实现网络内部的设备互联和对外部网络的访问。
- （5）实施网络安全策略：学会配置和实施基本的网络安全策略，包括防火墙设置、访问控制列表（ACL）的应用等，以确保网络的安全性。
- （6）优化网络性能：通过合理的带宽分配、设备优化和网络监控，优化校园网络的性能，确保流畅的数据传输和服务质量。
- （7）解决网络故障：学习使用思科模拟器进行故障排除，定位并解决网络中可能出现的常见问题，提高网络的可靠性和可维护性。
- （8）模拟实际场景：利用思科模拟器创建真实的校园网络场景，考虑到不同楼层、部门和设备类型的差异，以更好地模拟实际部署环境。

## 2. 设计内容

### 2.1 设计要求

实际应用中校园网涉及多个部门，本实验选择三个部门构建网络，一个教学部分，一个学生公寓部门，一个为数据中心，存放校园网 WEB 服务器；接入外网网段 IP 为 202.204.100.0/24，部分 IP 地址已经给出，正确配置网络设备，选择合适的路由协议，保证内网所有 PC 机均能连通外网，也就是 PC 能 ping 通路由器 Router1 的串口地址，外网主机能够访问内部 WEB 服务器。

在上述实现的基础上增加系统功能：

- （1）增加一个部门计通学院，校园内有 4 个部门：数据中心、教学区、学生公寓和计通学院；
- （2）在三层交换机上配置 DHCP，实现教学区、学生公寓和计通学院 3 个部门的主机能够自动获取 IP 地址；
- （3）出口路由器同时配置静态 NAT 和动态 NAT，静态 NAT 实现内部 WEB 服务器能够被外部主机访问，动态 NAT 实现内部主机能够访问互联网；
- （4）数据中心增加 DNS 服务器，实现校园网内部主机，能够通过域名访问 WEB 服务器；
- （5）数据中心增加 FTP 服务器，实现校园网内部主机，能够访问 FTP 文件服务器，实现文件下载服务；
- （6）选择所增加的计通学院部门分配 IPv6 地址，实现 IPv4 和 IPv6 在校园网中共存并且能通信。

### 2.2 设计实现

基于提出的设计要求，本项目进行了如下的设计实现。

- （1）设计实现了校园网，构建 4 个部门网络：教学区、学生公寓、计通学院和数据中心；
- （2）教学区、学生公寓和计通学院下各配置了 2 台主机来代表实际配置的主机进行测试；
- （3）数据中心配置了 3 台服务器：Web Server 网络服务器、DNS Server DNS 服务器和 FTP Server FTP 服务器；
- （4）本项目在外界配置 1 台主机代表外部网络，外部主机可以访问校园网内部的 Web 服务器；
- （5）三层交换机上配置了 DHCP，实现教学区、学生公寓和计通学院能够自动获取 IP 地址；
- （6）DNS 服务器为校园网内部主机提供域名服务，即主机可以通过域名访问校园网内的 Web 服务器；

- (7) FTP 服务器，实现校园网内部主机，能够访问 FTP 文件服务器，实现文件下载服务；
- (8) 在 IPv4 的基础上，配置 IPv6 相关信息，使得整个校园网内部可以同时使用 IPv4 和 IPv6 地址；
- (9) 绘制项目设计的网络拓扑结构图；
- (10) 出口路由器配置静态 NAT 和动态 NAT，静态 NAT 实现内部 WEB 服务器能够被外部主机访问，动态 NAT 实现内部主机能够访问互联网；

### 3. 实现步骤

#### 3.1 拓扑图设计

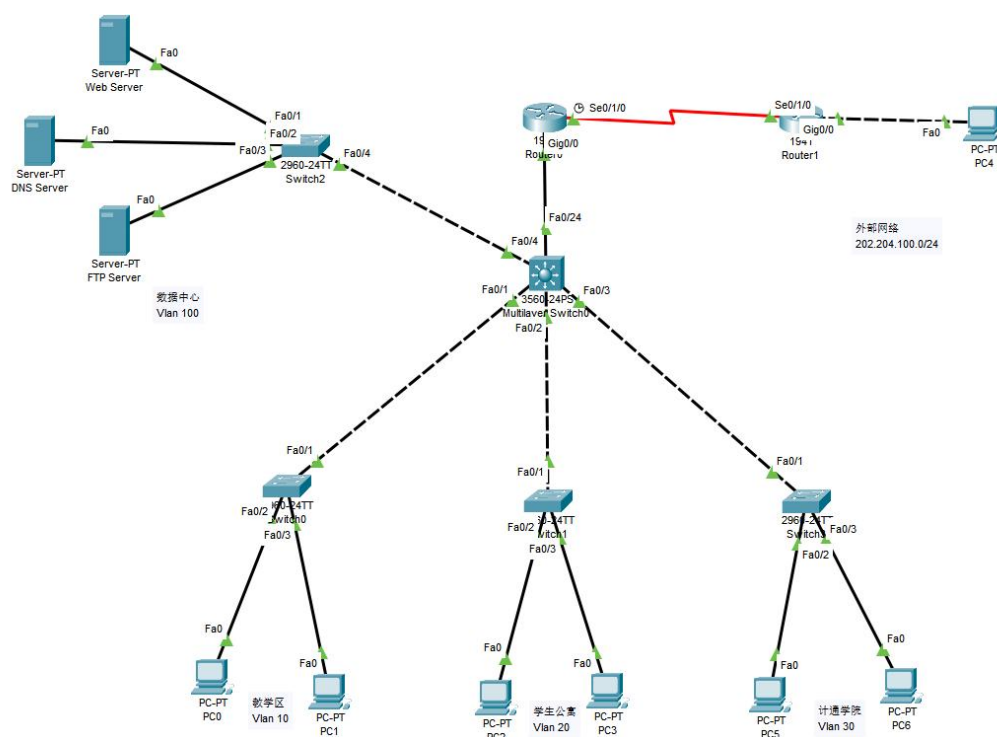


图 1 网络拓扑结构图

#### 3.2 IP 规划表

根据网络拓扑图及实验要求，在内网中规划了 5 个 Vlan，其中 Vlan10、Vlan20 和 Vlan30 分别用于教学区、学生公寓和计通学院；Vlan100 用于数据中心服务器区；Vlan110 用于核心交换机 Multilaver Switch0 和出口路由器 Router0 的互连。

公网 IP 地址分配情况如下：202.204.100.1-202.204.100.2 用于用户内外网路由器的接口地址；100.1.1.11 用于内网中 WEB 服务器的静态 NAT 地址映射；100.1.1.100-100.1.1.150 用于动态 NAT 的公网 IP 地址池；具体网络设备及终端的 IP 地址分配情况如下表。

表 1 网络终端地址规划表

设备	IP 地址	网关	VLAN
PC0	192.168.10.2	192.168.10.1	10
PC1	192.168.10.3	192.168.10.1	10

PC2	192.168.20.2	192.168.20.1	20
PC3	192.168.20.3	192.168.20.1	20
PC4	10.1.1.11	10.1.1.1	无
PC5	192.168.30.2	192.168.30.1	30
PC6	192.168.30.3	192.168.30.1	30
Web Server	192.168.100.11	192.168.100.1	100
DNS Server	192.168.100.22	192.168.100.1	100
FTP Server	192.168.100.33	192.168.100.1	100

应该注意到，上表中的 PC0-3 和 PC5-6 的 IP 信息是通过 DHCP 自动获取的，在这里只是进行了集中展示，并不代表使用的静态 IP。

表 2 网络设备端口地址规划表

设备	端口	IP 地址
Multilaver Switch0	Fa0/1	192.168.10.1
	Fa0/2	192.168.20.1
	Fa0/3	192.168.30.1
	Fa0/4	192.168.100.1
	Fa0/24	192.168.110.1
Router0	Gig0/0	192.168.110.2
	Se0/1/0	202.204.100.1
Router1	Se0/1/0	202.204.100.2
	Gig0/0	10.1.1.1

在上表中，Multilaver Switch0 的 Fa0/24 与 Router0 的 Gig0/0 相连；Router0 的 Se0/1/0 与 Router1 的 Se0/1/0 相连。

表 3 网络地址转换 NAT 地址映射表

设备	内网地址	公网地址
Web 服务器	192.168.100.11	100.1.1.11
PC0	192.168.10.2	100.1.1.100-100.1.1.150 地址池

PC1	192.168.10.3	100.1.1.100-100.1.1.150 地址池
PC2	192.168.20.2	100.1.1.100-100.1.1.150 地址池
PC3	192.168.20.3	100.1.1.100-100.1.1.150 地址池
PC5	192.168.30.2	100.1.1.100-100.1.1.150 地址池
PC6	192.168.30.3	100.1.1.100-100.1.1.150 地址池

### 3.3 主要技术

#### 3.3.1 VLAN 间通信技术

虚拟局域网（VLAN）间通信技术是一种网络设计方法，旨在实现在物理网络基础上的逻辑网络划分。VLAN 是通过将网络设备（如交换机）上的端口分组，使得它们可以被视为一个独立的逻辑网络，与同一 VLAN 内的设备通信。然而，VLAN 间通信技术允许不同 VLAN 内的设备进行跨网络的通信。

一种常见的 VLAN 间通信技术是使用三层交换机或者路由器。这些设备能够理解和转发不同 VLAN 的数据包，从而实现不同虚拟网络之间的通信。通常，这可以通过在交换机或路由器上配置子接口，每个子接口代表一个 VLAN，并分配相应的 IP 地址。

VLAN 间通信技术还可以通过使用三层交换机上的 Inter-VLAN 路由功能来实现。这意味着三层交换机能够直接路由不同 VLAN 之间的流量，而无需外部路由器。这种方法可以提高网络性能和减少网络拓扑的复杂性。

VLAN 间通信技术的优势包括提高网络的灵活性和可管理性，允许根据不同的业务需求对网络进行逻辑划分。然而，为确保安全性和网络性能，需要仔细规划和配置 VLAN，并实施适当的安全措施，如访问控制列表（ACL）和虚拟局域网的隔离。

#### 3.3.2 网络路由配置

新的路由器中没有任何地址信息，路由表也是空的，路由都是通过路由协议来学习到的。根据路由器学习路由的方法不同，路由可分为直连路由、静态路由和动态路由 3 种。

直连路由无需配置，是路由器根据网络结构自学到的。所谓静态路由，是指网络管理员根据其所掌握的网络连通信息，以手工配置方式来添加路由到路由器的 IP 路由表中。默认路由是一种特殊的静态路由，指的是当路由表中与包的目的地址之间没有匹配的表项时路由器能够做出的选择。静态路由指令在中小型网络组建中较为常见。在大规模网络中，希望有一种能自动适应网络状态变化，而对路由表信息进行动态更新和维护的路由生成方式，这就是动态路由。常见的动态路由协议包括 R IP、OSPF、IS-IS、IG R P、EIG R P、BGP 等。



### 3.3.3 NAT 技术

网络地址转换（NAT）技术是一种在计算机网络中常用的技术，旨在解决 IPv4 地址短缺的问题以及提供一层安全性。NAT 允许在私有网络内使用非注册的 IP 地址，并通过将这些私有地址映射到一个或多个公共 IP 地址来实现对外通信。

（1）地址转换：NAT 主要通过私有网络内使用私有 IP 地址，然后在数据包离开私有网络时将这些私有 IP 地址转换为一个或多个公共 IP 地址，从而实现对外通信。这有效地缓解了 IPv4 地址短缺问题。

（2）类型：NAT 有不同的类型，包括静态 NAT、动态 NAT 和 PAT（端口地址转换）。静态 NAT 映射固定的私有 IP 地址到公共 IP 地址，而动态 NAT 和 PAT 使用动态映射，允许多个私有 IP 地址共享一个或少量的公共 IP 地址。

（3）安全性：NAT 提供了一定程度的安全性，因为在私有网络内使用私有 IP 地址，这使得内部网络结构对外部网络不可见。这种隐蔽性有助于防范一些网络攻击，尽管 NAT 并非专门设计用于安全目的。

### 3.3.4 静态路由配置

静态路由配置是在计算机网络中一种简单而有效的路由管理方法，通过手动配置网络管理员指定的路由信息来控制数据包的转发。在静态路由中，路由表的项是由管理员直接定义的，不依赖于动态路由协议的自动更新。

（1）手动配置路由表：网络管理员通过手动输入路由信息，指定目的网络及其关联的下一跳路由器或出口接口。这种方式适用于相对简单的网络环境，或者在特定需求下需要精确控制路由的情况。

（2）适用于小型网络：静态路由常用于小型网络或者需要维护简单路由关系的场景，例如连接少数网络设备的小型办公室网络。在这些情况下，手动配置提供了一种直观且易于管理的方法。

（3）稳定性和可预测性：静态路由的配置使网络更加稳定，因为路由表的更新不依赖于网络拓扑的动态变化。这提供了可预测的路由行为，不受网络拓扑变化的影响。

### 3.3.5 IPv4 与 IPv6 共存

IPv4 与 IPv6 共存是一种网络演进的策略，旨在平滑地过渡到 IPv6，并使 IPv6 和 IPv4 能够在同一网络中共存运行。由于 IPv4 地址枯竭和 IPv6 的广泛推广，许多组织正在逐渐采用 IPv6，但由于 IPv4 仍然是互联网上广泛使用的协议，实现 IPv4 与 IPv6 的共存是至关重要的。

在 IPv4 与 IPv6 共存的环境中，网络设备和应用程序需要同时支持 IPv4 和 IPv6 协议。这涉及到在路由器、交换机、防火墙等网络设备上配置双协议支持，并确保应用程序能够正确处理 IPv4 和 IPv6 地址。

一种常见的 IPv4 与 IPv6 共存的实现方式是双协议栈，即同时运行 IPv4 和 IPv6 协议栈。这允许设备在 IPv4 和 IPv6 网络中都能正常工作。此外，还可以使用隧道技术，如 6to4 和 ISATAP，来在 IPv4 网络上运输 IPv6 流量。

### 3.3.6 DHCP 技术

动态主机配置协议（DHCP）技术是一种网络协议，旨在自动分配 IP 地址和其他网络配置信息给计算机网络中的设备。DHCP 简化了网络管理，允许设备在连接到网络时自动获取所需的网络参数，如 IP 地址、子网掩码、网关和 DNS 服务器地址等。DHCP 采用客户端-服务器模型，其中 DHCP 服务器负责分配 IP 地址，而设备作为 DHCP 客户端主动请求这些地址。

（1）自动地址分配：DHCP 通过自动分配 IP 地址，避免了手动配置每个设备的繁琐过程。这对于大型网络尤其重要，以确保网络上的设备都能够有效地获得可用的 IP 地址。

（2）动态更新：DHCP 支持动态更新，允许设备在网络中移动或连接到其他网络时自动获取新的配置信息，而无需手动重新配置。这提高了网络的灵活性和可管理性。

### 3.3.7 DNS 技术

DNS 技术是一种关键的因特网基础设施，旨在将易于记忆的域名映射到计算机网络中的 IP 地址。在互联网上，每个设备都有一个唯一的 IP 地址，而 DNS 作为一种分布式数据库系统，提供了域名到 IP 地址之间的映射服务，使用户能够通过人类可读的域名访问互联网资源。

DNS 的工作原理是通过层级的域名体系，将域名划分为若干级别，例如顶级域名（TLD）和二级域名。当用户在浏览器中输入域名时，本地 DNS 解析器首先查询本地缓存，如果未找到，则向根域名服务器查询。根服务器指导解析器进一步查询相应的顶级域名服务器，然后逐级向下，直到找到负责该域名的权威域名服务器。最终，权威域名服务器返回与该域名关联的 IP 地址，使得用户的请求得以满足。

### 3.3.8 FTP 技术

FTP 技术是一种用于在计算机网络上传输文件的标准协议。FTP 允许用户将文件从一个计算机（FTP 客户端）传输到另一个计算机（FTP 服务器），或者从服务器下载文件到客户端。这一协议提供了一种简单而有效的方式，使得文件在网络上的传输变得可靠且高效。

FTP 工作在客户端-服务器模型下，其中客户端通过使用 FTP 客户端软件与服务器建立连接，并发送 FTP 命令来请求文件的传输。用户可以通过明文模式（不加密）或加密模式（如 FTP over TLS/SSL）进行文件传输，根据安全需求选择适当的方式。

### 3.4 设备配置

#### 3.4.1 DHCP 相关配置

为实现 DHCP，需要重点对交换机 Multilaver Switch0 进行配置，兼顾对 Switch0-1、Switch3 的配置，配置完成时主机将自动获得 IP 地址信息，相关配置的关键代码如下。

表 4 Switch0 关键配置命令

```
en
conf ter
vlan 10
exit
//划分 vlan
int range F0/2-3
switch mode access
switch access vlan 10
no shut
exit
int F0/1
switch mode trunk
switch trunk allowed vlan 10
no shut
exit
```

表 5 Switch1 关键配置命令

```
en
conf ter
vlan 20
exit
//划分 vlan
int range F0/2-3
switch mode access
switch access vlan 20
no shut
exit
int F0/1
switch mode trunk
switch trunk allowed vlan 20
no shut
exit
```

表 6 Switch3 关键配置命令

```
en
conf ter
vlan 30
exit
//划分 vlan
int range F0/2-3
switch mode access
switch access vlan 30
no shut
exit
int F0/1
switch mode trunk
switch trunk allowed vlan 30
no shut
exit
```

表 7 Multilaver Switch0 关键配置命令

```
en
conf ter
vlan 10
vlan 20
vlan 30
//配置 vlan10
int F0/1
switch trunk allowed vlan 10
exit
ip dhcp excluded-address 192.168.10.1
int vlan 10
ip address 192.168.10.1 255.255.255.0
ip routing
exit
ip dhcp pool 10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
exit
//配置 vlan20
int F0/2
switch trunk allowed vlan 20
exit
ip dhcp excluded-address 192.168.20.1
int vlan 20
ip address 192.168.20.1 255.255.255.0
ip routing
exit
ip dhcp pool 20
```

```
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
exit
//配置 vlan30
int F0/3
switch trunk allowed vlan 30
exit
ip dhcp excluded-address 192.168.30.1
int vlan 30
ip address 192.168.30.1 255.255.255.0
ip routing
exit
ip dhcp pool 30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
exit
```

完成上述配置后，校园网内主机 PC0-3 和 PC5-6 中开启 DHCP 动态获取 IP，可以看到几秒钟过后成功自动获取 IP。

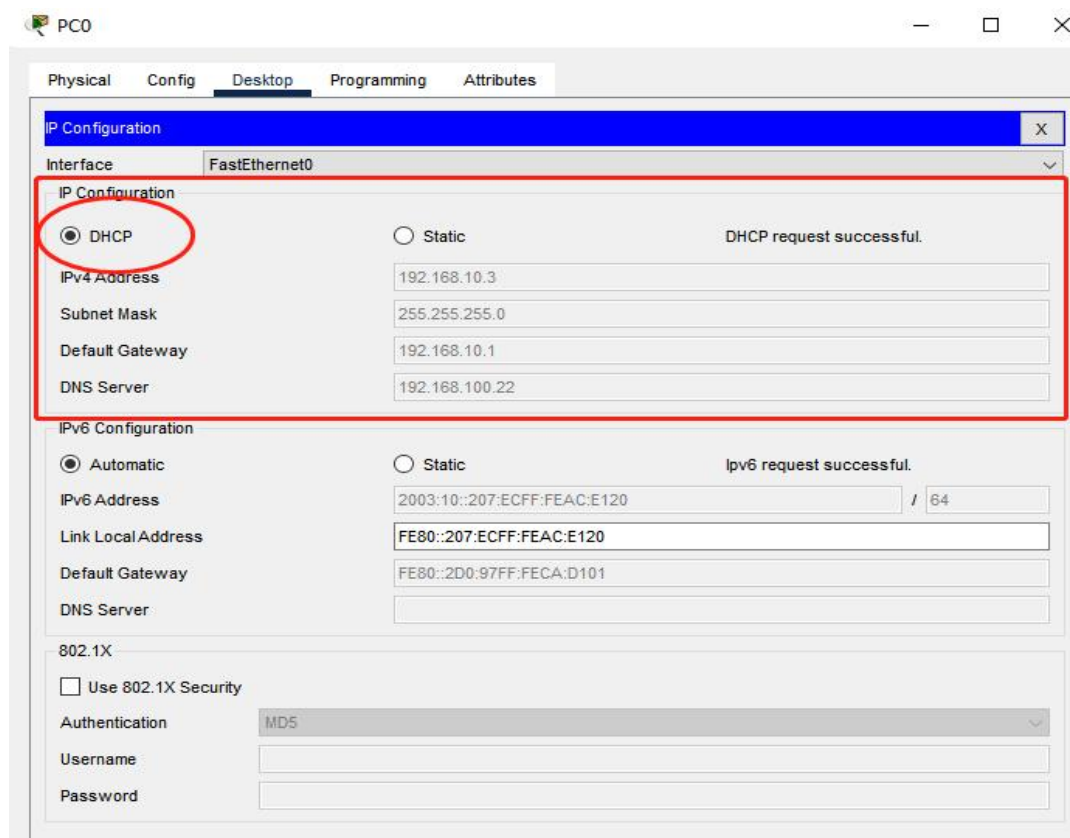


图2 主机通过 DHCP 获取 IP 示意图

### 3.4.2 数据中心基本配置

在这一环节，主要需要配置交换机 Switch2、数据中心的 3 台服务器和核心交换机 Multilayer Switch0，相关关键配置命令如下。

表 8 Switch2 关键配置命令

```
en
conf ter
vlan 100
exit
//划分 vlan
int range F0/1-3
switch mode access
switch access vlan 100
no shut
exit
int F0/4
switch mode trunk
switch trunk allowed vlan 100
no shut
exit
```

表 9 Multilayer Switch0 关键配置命令

```
en
conf ter
vlan 100
int F0/4
//配置 vlan
switch mode trunk
switch trunk allowed vlan 100
no shut
int vlan 100
ip address 192.168.100.1 255.255.255.0
exit
```

按照 IP 规划表中的内容对 Web 服务器、DNS 服务器和 FTP 服务器进行配置，使用静态 IP，通过图形化界面进行，简单方便。

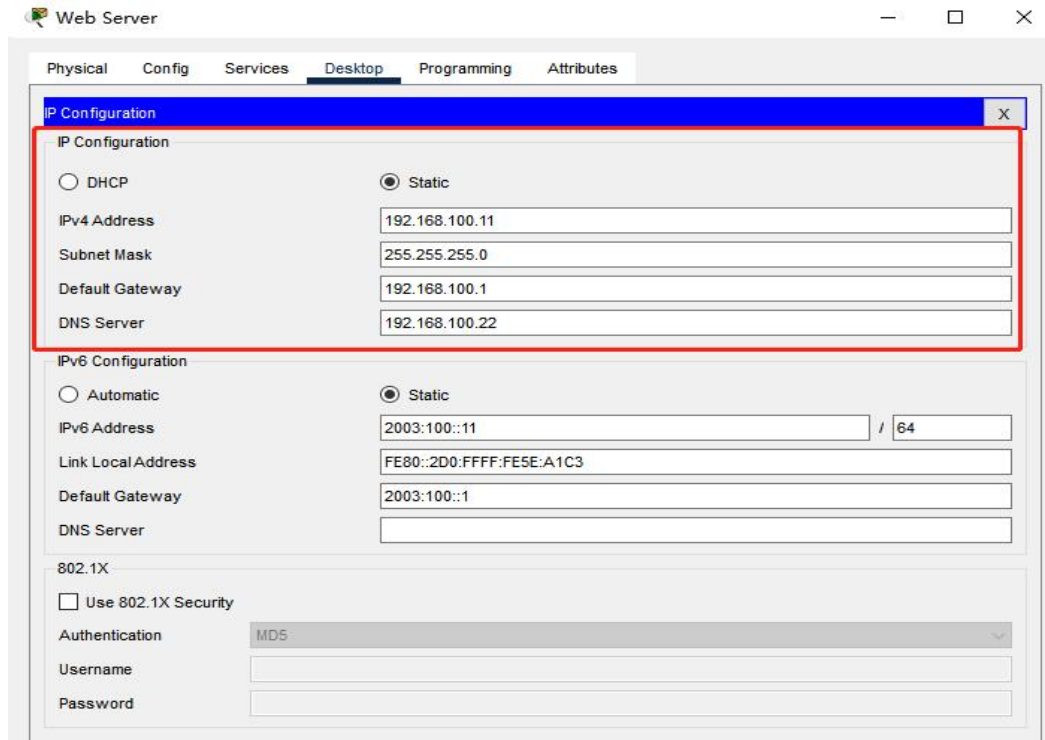


图 3 Web 服务器 IP 配置示意图

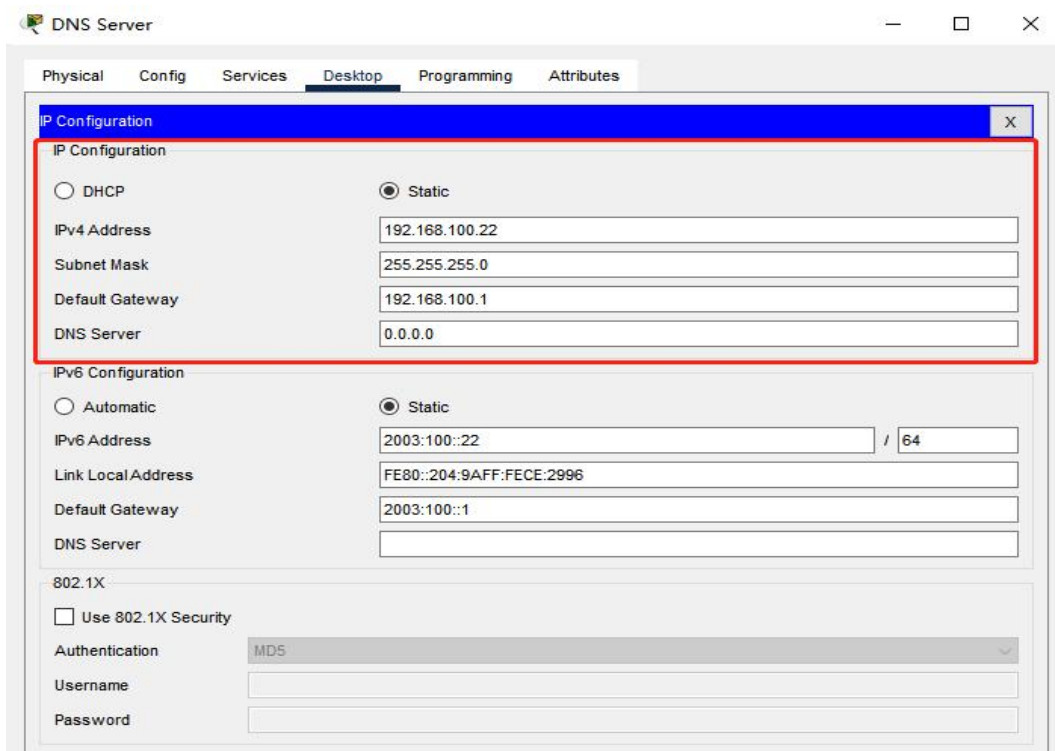


图 4 DNS 服务器 IP 配置示意图

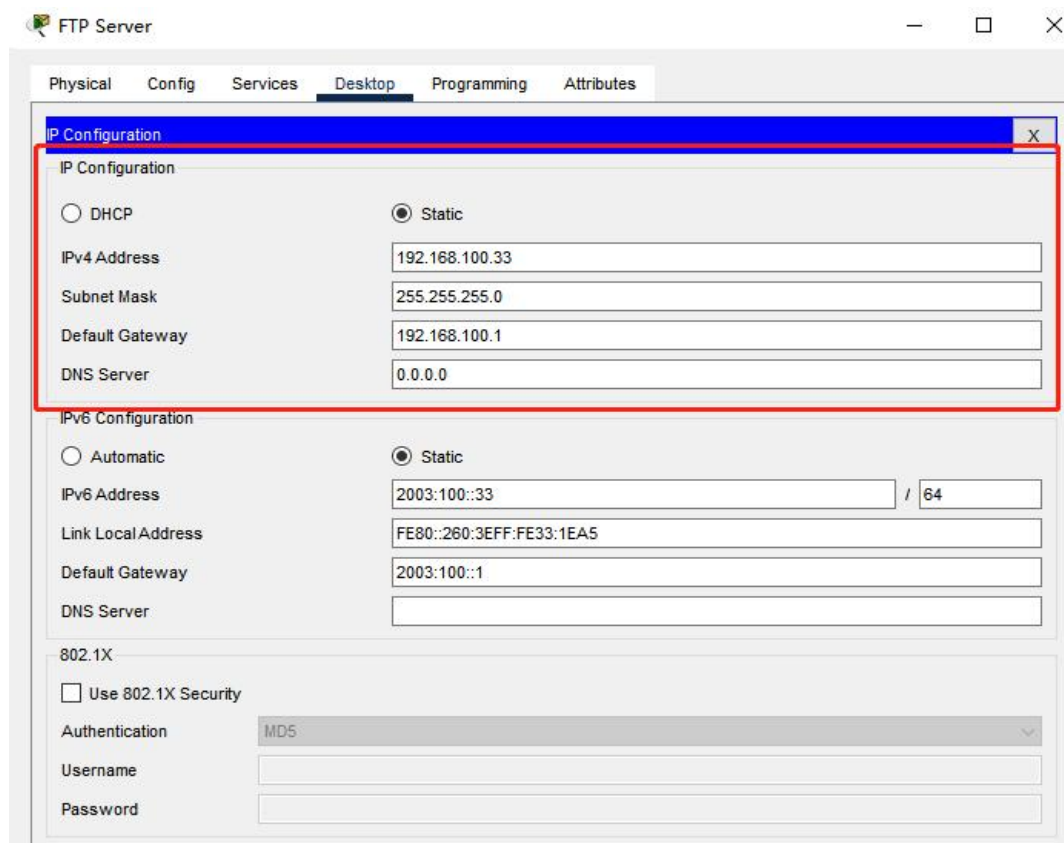


图 5 FTP 服务器 IP 配置示意图

### 3.4.3 外网基本配置

在这一环节，主要需要对核心路由器 Multilayer Switch0、边界路由器 Router0、外界路由器 Router1 和外界主机 PC4 进行配置。具体配置均按照 IP 规划表中的信息进行配置，相关关键配置命令如下。

表 10 Multilayer Switch0 关键配置命令

```
en
conf ter
vlan 110
exit
int F0/24
switch access vlan 110
no shut
exit
int vlan 110
ip address 192.168.110.1 255.255.255.0
exit
```



表 11 Router0 关键配置命令

```
en
conf ter
int Gig0/0
ip address 192.168.110.2 255.255.255.0
no shut
exit
int Ser0/1/0
ip address 202.204.100.1 255.255.255.0
clock rate 64000
no shut
exit
```

表 12 Router1 关键配置命令

```
en
conf ter
int Ser0/1/0
ip address 202.204.100.2 255.255.255.0
clock rate 64000
no shut
exit
int Gig0/0
ip address 10.1.1.1 255.255.255.0
no shut
exit
```

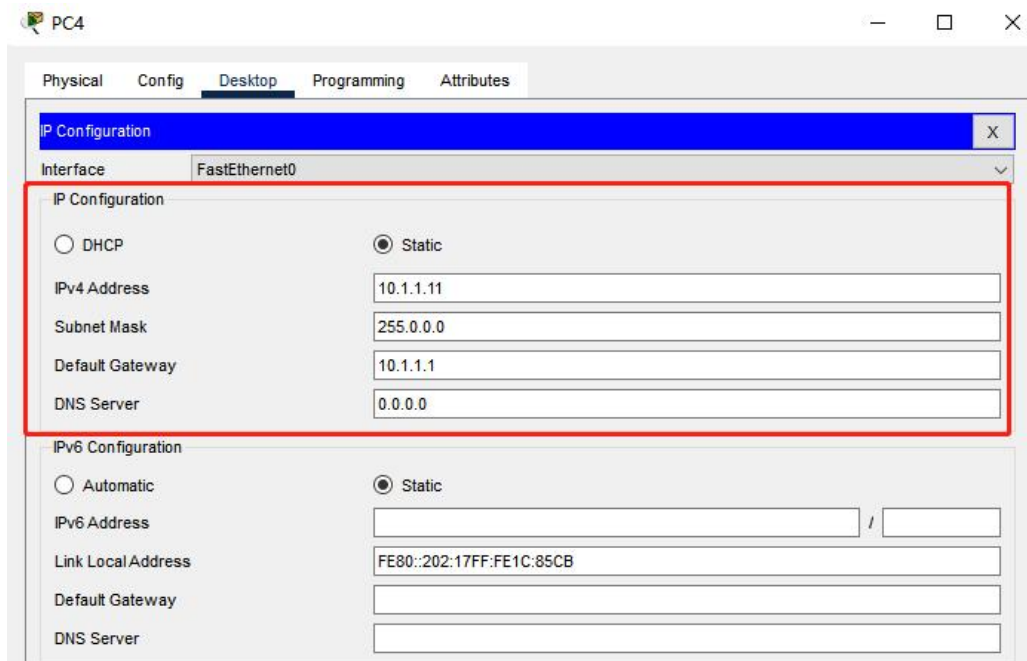


图 6 外网主机 PC4 配置示意图

### 3.4.4 路由配置

在这一环节，主要需要对核心交换机 Multilayer Switch0、边界路由器 Router0 和外界路由器 Router1 进行路由配置，实现最基本的通信功能：内网主机访问外部网络，外网主机访问内部 Web 服务器。在后续会对相关路由器其进行 NAT 配置，实现网络地址转换功能。

表 13 Multilayer Switch0 关键配置命令

```
en
conf ter
ip route 0.0.0.0 0.0.0.0 192.168.110.2
ip routing
```

表 14 Router0 关键配置命令

```
en
conf ter
ip route 0.0.0.0 0.0.0.0 202.204.100.2
ip route 192.168.10.0 255.255.255.0 192.168.110.1
ip route 192.168.20.0 255.255.255.0 192.168.110.1
ip route 192.168.30.0 255.255.255.0 192.168.110.1
ip route 192.168.100.0 255.255.255.0 192.168.110.1
ip routing
```

表 15 Router1 关键配置命令

```
en
conf ter
ip route 192.168.100.0 255.255.255.0 202.204.100.1
ip route 100.1.1.11 255.255.255.0 202.204.100.1
ip routing
```

### 3.4.5 NAT 配置

在出口路由器 Router0 上进行配置 NAT 的关键代码如下，实现静态 NAT 和动态 NAT。

表 16 Router0 关键配置命令

```
en
conf ter
//静态 NAT 配置
ip nat inside source static 192.168.100.11 100.1.1.11
//动态 NAT 配置
ip nat pool netpool 100.1.1.100 100.1.1.150 netmask 255.255.255.0
access-list 10 permit 192.168.10.0 0.0.0.255
```

```
access-list 10 permit 192.168.20.0 0.0.0.255
access-list 10 permit 192.168.30.0 0.0.0.255
ip nat inside source list 10 pool natpool
//将配置策略应用到对应的端口
int Gig0/0
ip nat inside
exit
int Ser0/1/0
ip nat outside
exit
```

### 3.4.6 DNS 服务器配置

为校园网内的各主机配置 DNS 服务器，使得主机能够通过域名访问 Web 服务器。为此，需要在数据中心配置 Web 服务器开启 DNS 服务、Web 服务器配置 DNS 服务器、主机配置 DNS 服务器，相关配置过程如下。

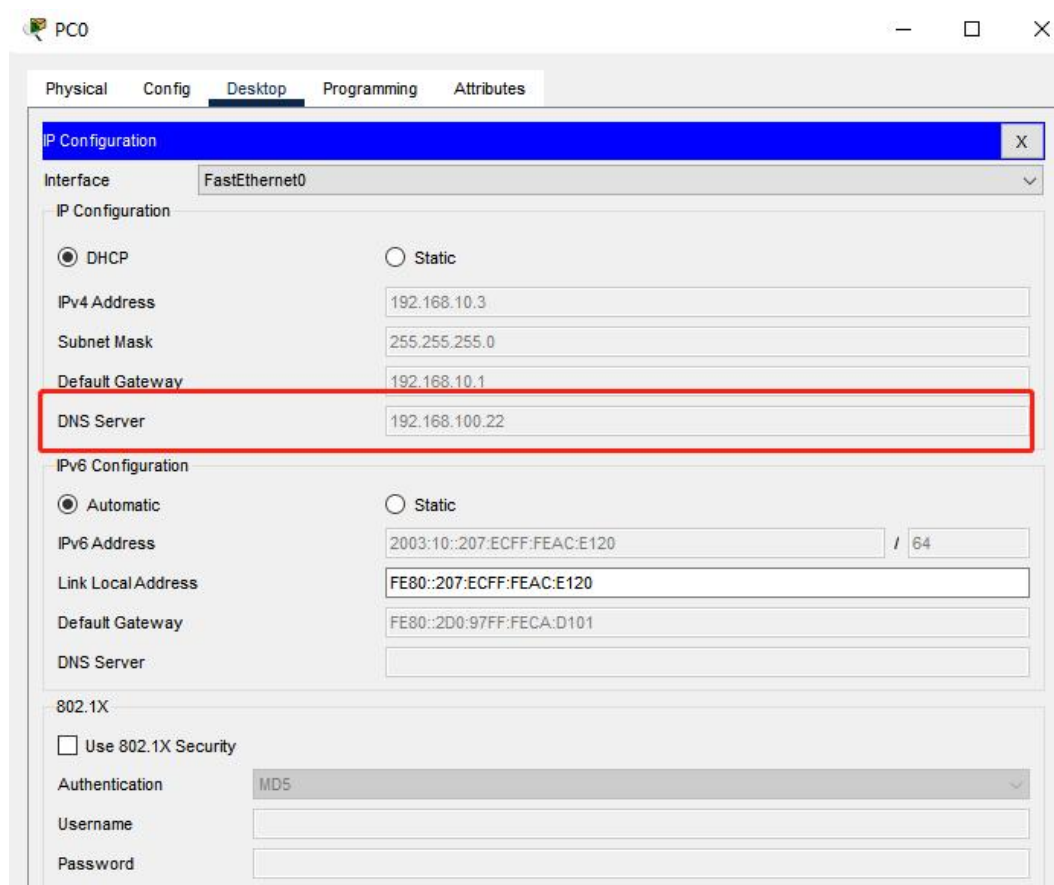


图 7 主机配置示意图

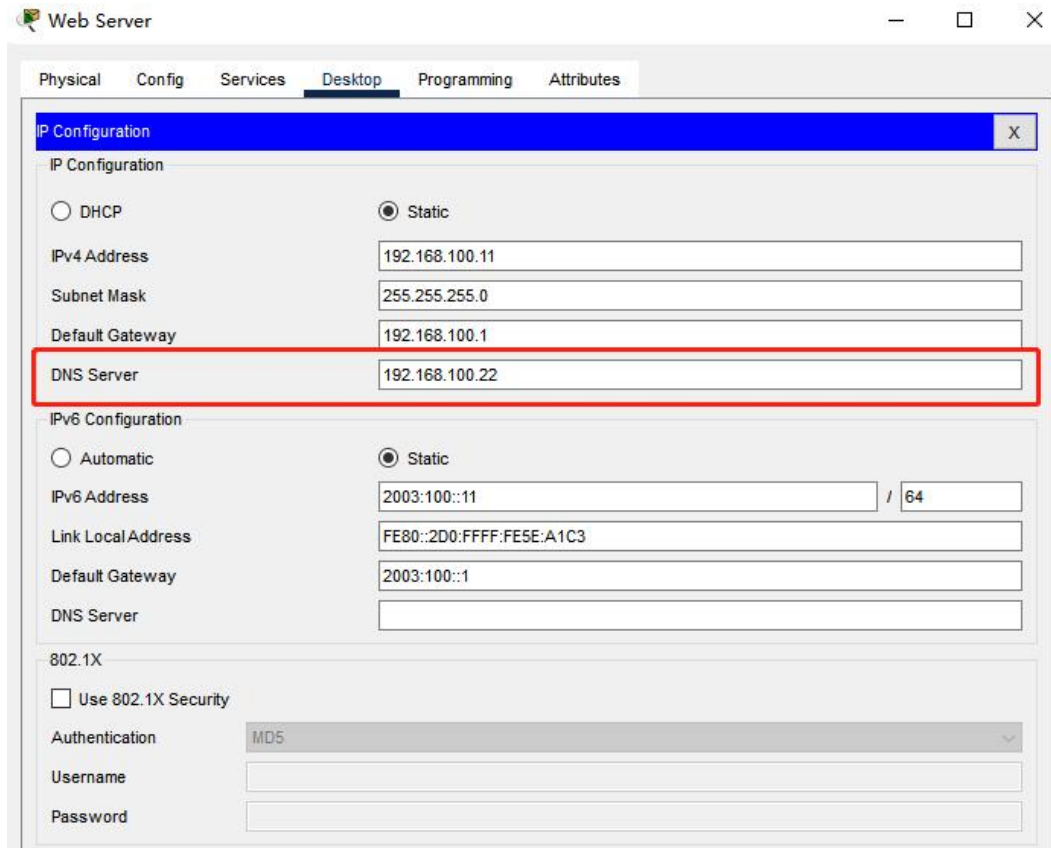


图 8 Web 服务器配置示意图

在 DNS 服务器中，开启 DNS 服务，并添加相应的记录，在这里我添加了为 Web 服务器添加域名 “www.ustb.edu.cn” 和 “www.baidu.com”。

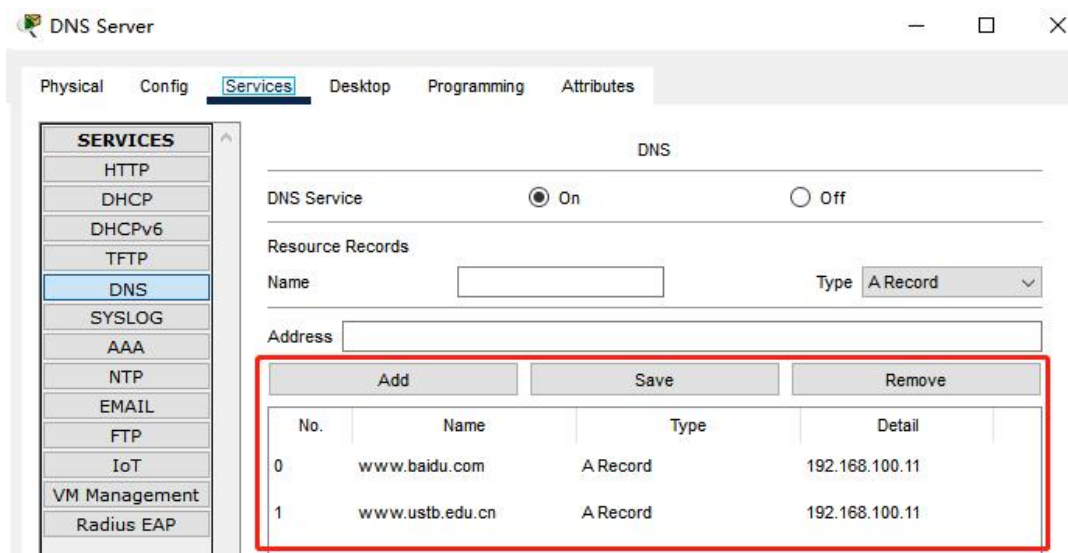


图 9 DNS 服务器配置示意图

### 3.4.7 FTP 服务器配置

在数据中心的配置 FTP 服务器，为主机提供文件下载。需要在 FTP 服务器中开启 FTP 服务，并添加相应的账户信息。在这里，我添加了：（1）管理员 admin，具备所有权限；（2）学生 student，只读权限；（3）教师 teacher，读写权限。

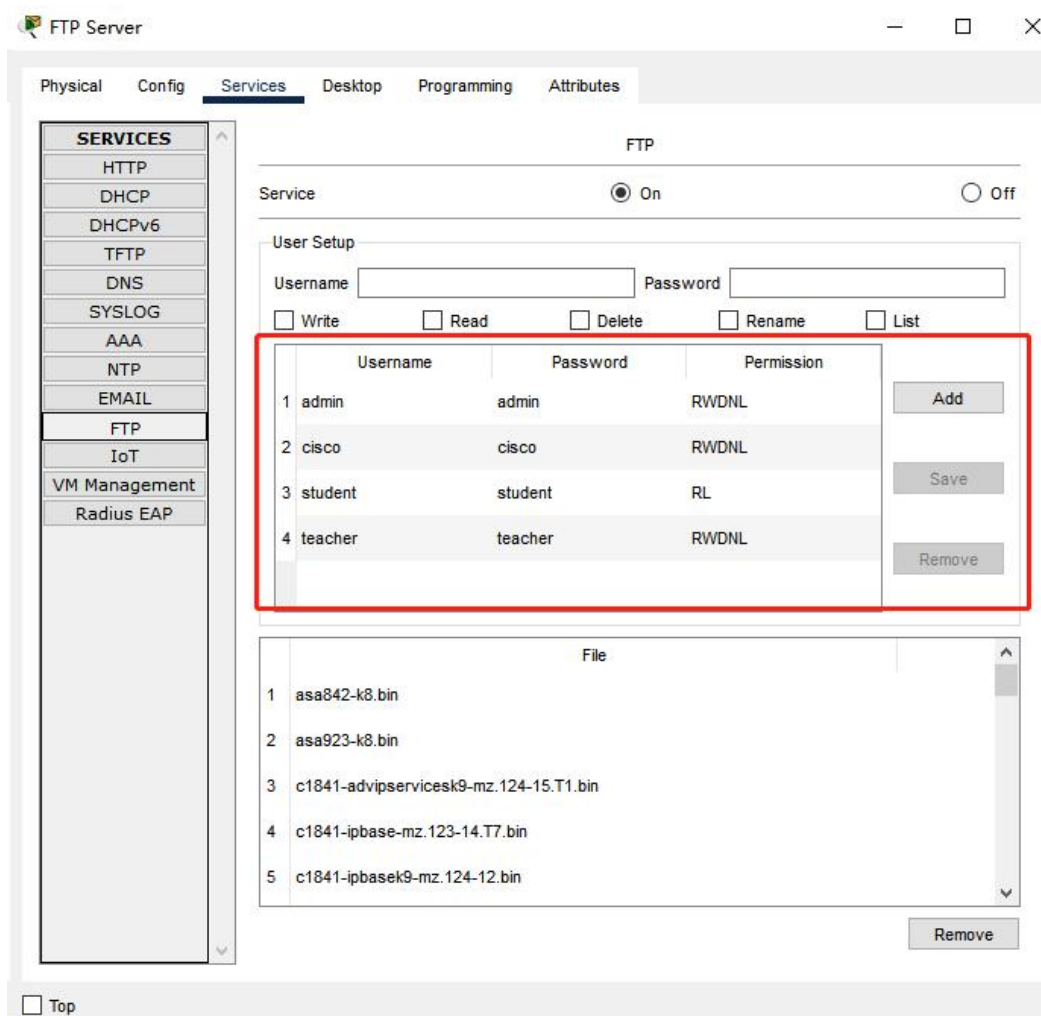


图 10 FTP 服务器配置示意图

### 3.4.8 IPv6 实现

在整个校园网内部实现 IPv6，使得校园网内部 IPv4 和 IPv6 共存，每个设备同时拥有 IPv4 和 IPv6 地址，且能够相互通信。主要需要配置接入交换机 Switch0-3 和核心交换机 Multilayer Switch0，另外为各个终端配置 IPv6 地址。

表 17 Multilayer Switch0 关键配置命令

```
en
conf ter
//开启 IPv6
sdm prefer dual-ipv4-and-ipv6 default
int vlan 10
ipv6 address 2003:10::1/64
no shut
exit
int vlan 20
ipv6 address 2003:20::1/64
no shut
exit
int vlan 30
ipv6 address 2003:30::1/64
no shut
exit
int vlan 100
ipv6 address 2003:100::1/64
no shut
exit
```

表 18 Switch0-3 关键配置命令

```
en
conf ter
//开启 IPv6
sdm prefer dual-ipv4-and-ipv6 default
```

进行上述配置后，将交换机进行重启，IPv6 开始工作。另外，需要对校园网内各个终端配置 IPv6 信息，使得校园网内部能够使用 IPv6 进行通信。相关配置情况如下。

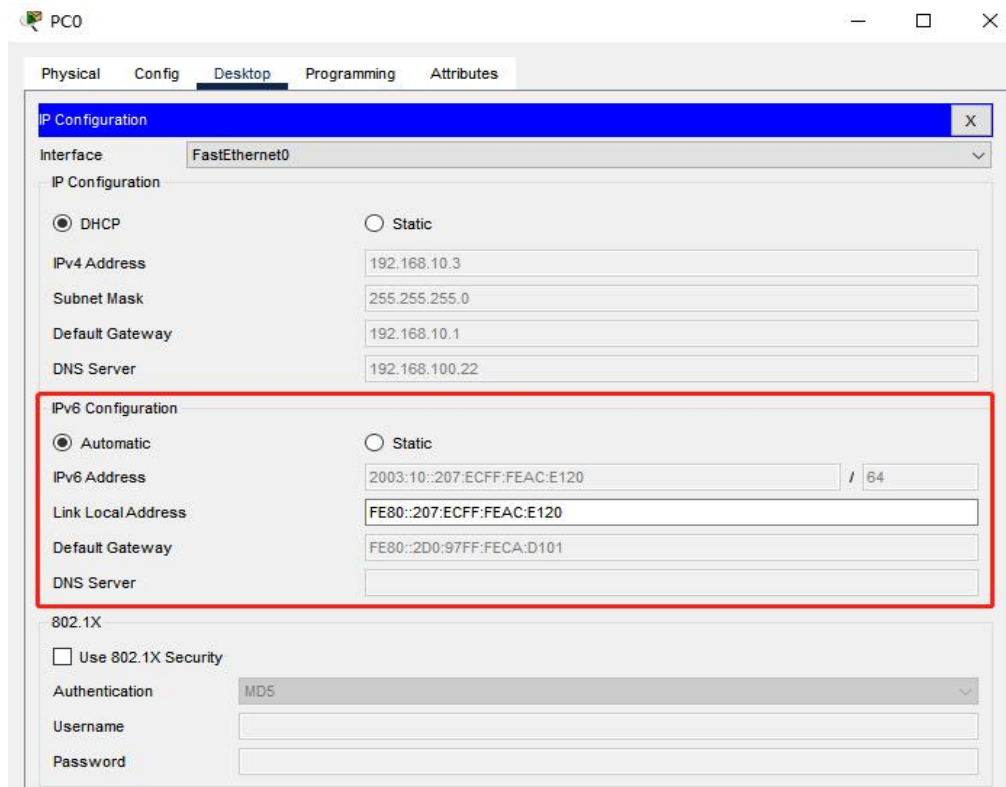


图 11 主机终端配置情况示意图

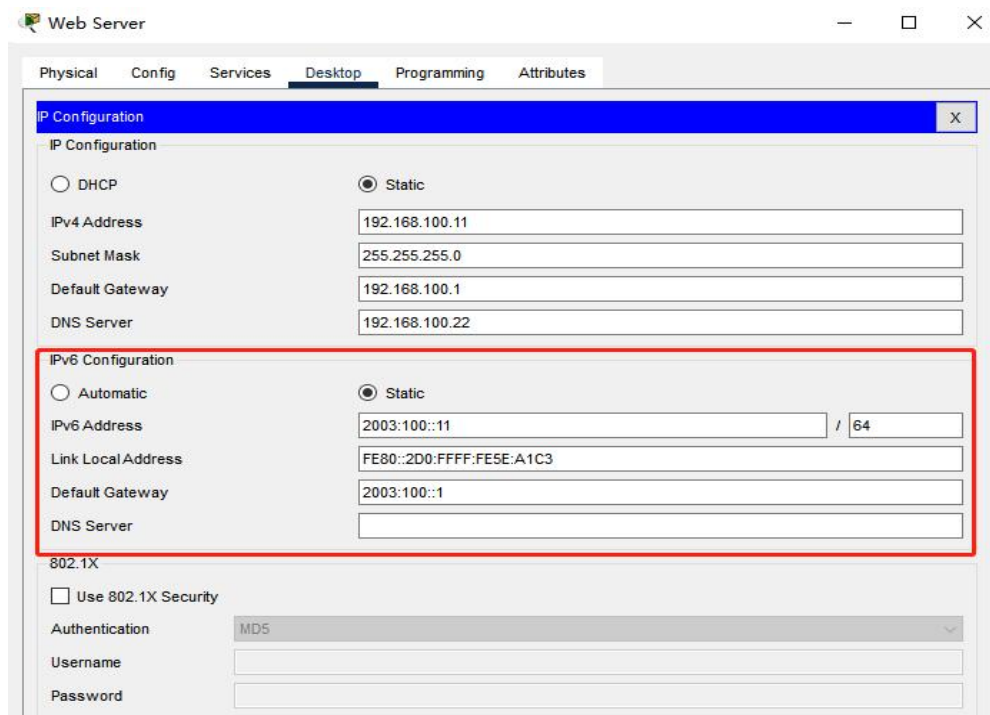


图 12 服务器终端配置情况示意图

### 3.5 测试验证

#### 3.5.1 基本连通测试

基本连通要求实现校园网内部终端能够访问外部网络，即 ping 通外部路由器 Router1 的串口端；外部网络终端能够访问校园网内部的 Web 服务器。经测试配置成功。

(1) 校园网内部终端以 PC0 为例，成功 ping 通外部路由器 Router1 串口端。

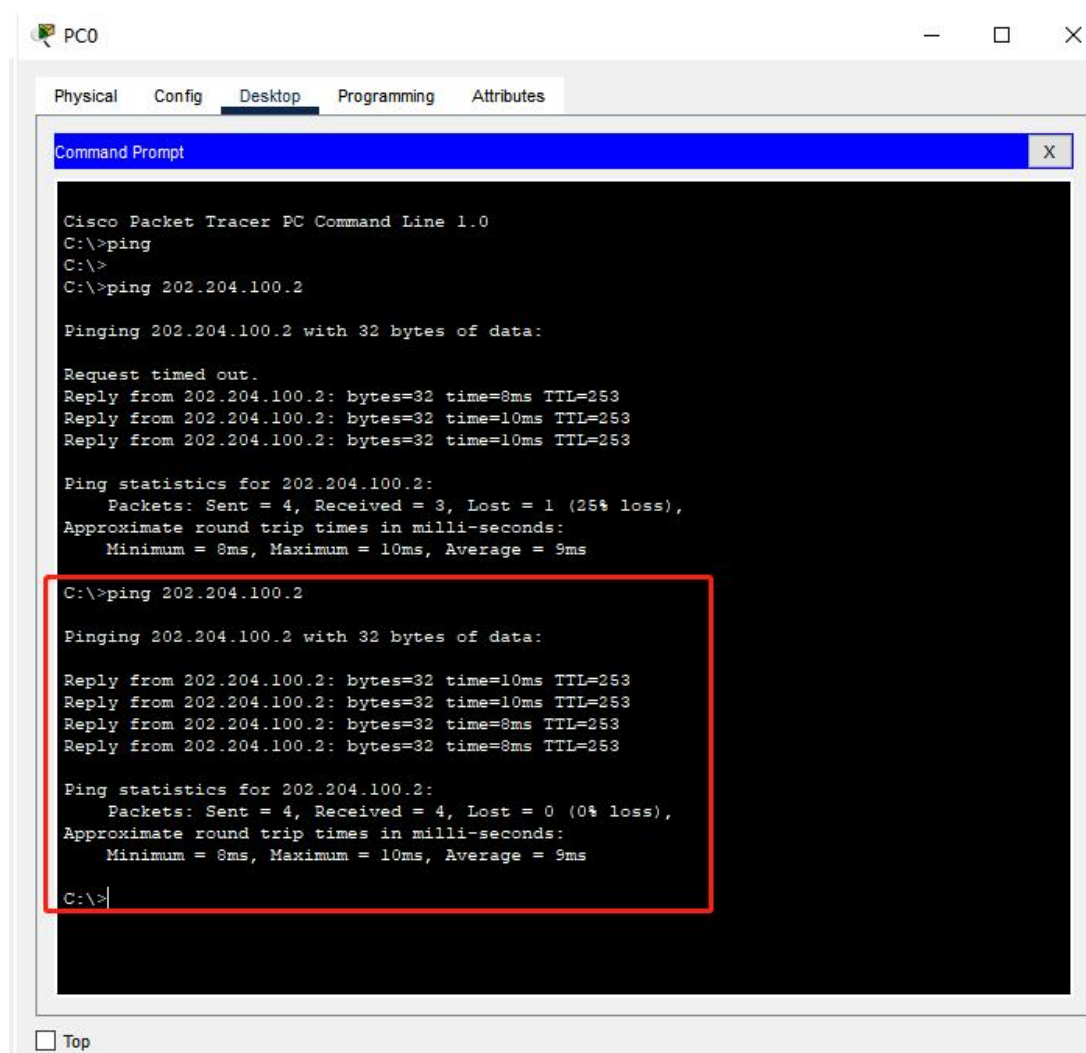


图 13 PC0 连通外部网络

(2) 外部网络终端以 PC4 为例，能够成功 ping 通 Web 服务器。



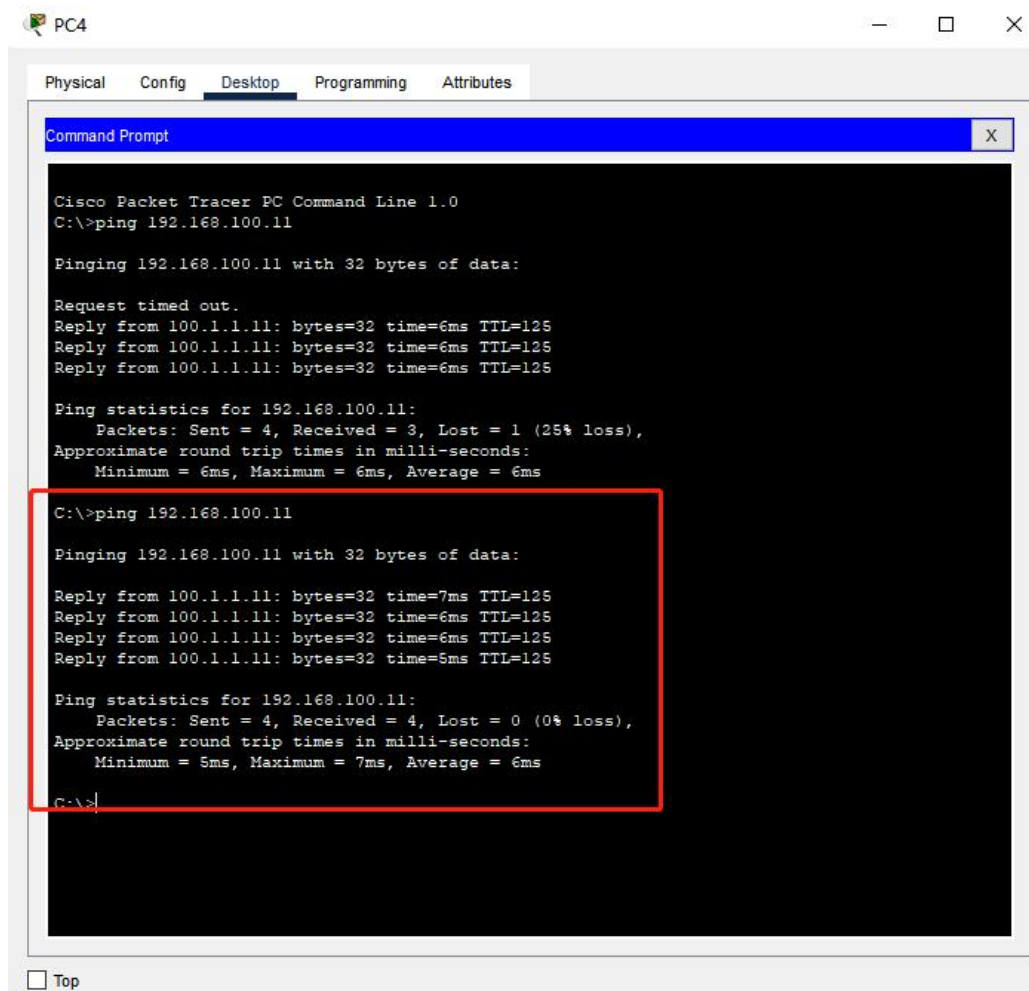


图 14 PC4 连通 Web 服务器

### 3.5.2 DHCP 配置测试

DHCP 配置要求接入网络的主机能够自动获取 IP 地址，测试情况如下：（1）PC 刚接入网络时没有有效 IP 地址；（2）经过一段时间后 PC 通过 DHCP 自动获取到有效 IP 地址。经测试配置成功。

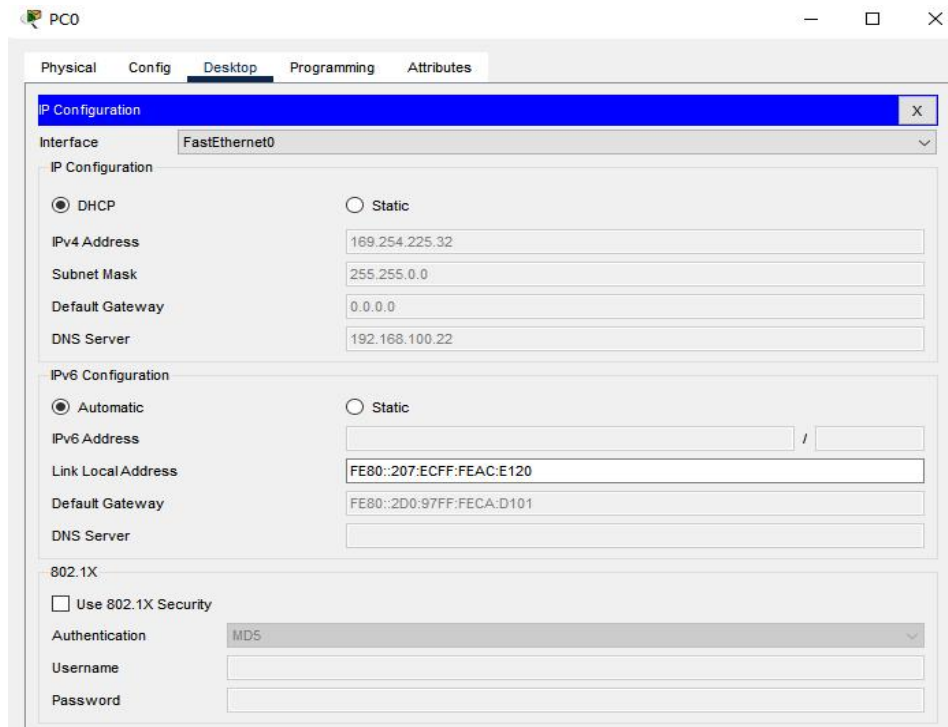


图 15 PC 未获取 IP 图

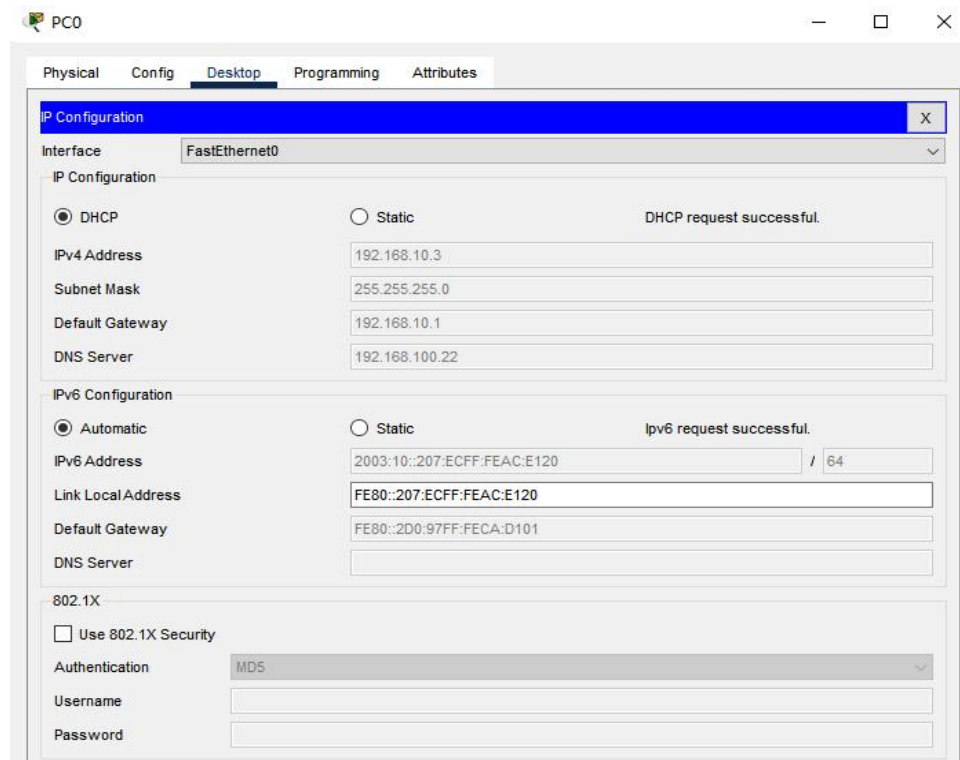


图 16 PC 通过获得有效 IP 图

### 3.5.3 NAT 配置测试

NAT 配置测试需要测试静态 NAT 和动态 NAT。

(1) 在外网 PC4 中使用 ping 指令测试 Web 服务器的公网地址 100.1.1.11 连通性的同时，在边界路由器 Router0 用 debug ip nat 测试，验证配置成功。

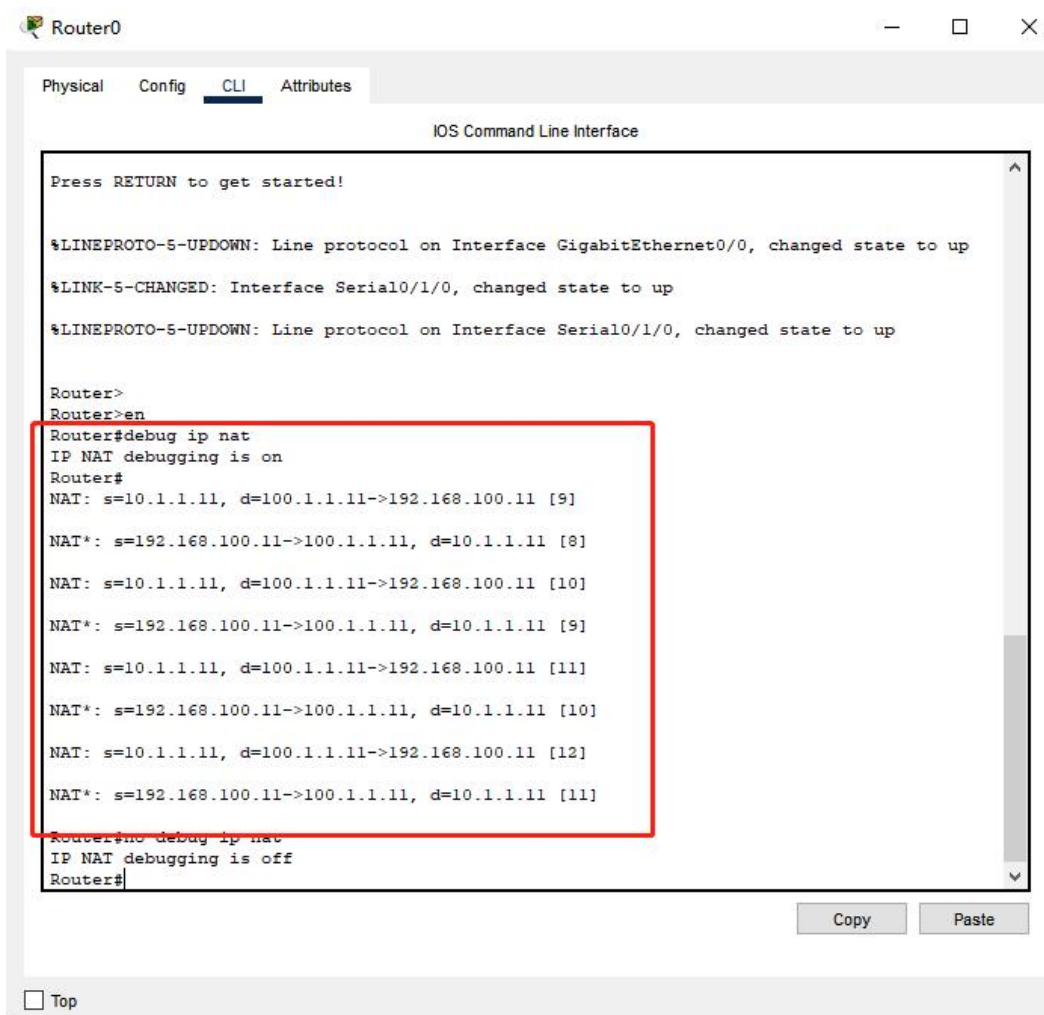


图 17 静态 NAT 验证

(2) 在内网 PC0 执行 ping 指令，测试与外网的连通性的同时，在边界路由器 Router0 上通 show ip nat translations 查看地址转换情况，验证配置成功。

The screenshot shows the Cisco Router CLI interface for Router0. The CLI tab is selected. The output shows the following commands and results:

```

Router>
Router>en
Router#debug ip nat
IP NAT debugging is on
Router#
NAT: s=10.1.1.11, d=100.1.1.11->192.168.100.11 [9]
NAT*: s=192.168.100.11->100.1.1.11, d=10.1.1.11 [8]
NAT: s=10.1.1.11, d=100.1.1.11->192.168.100.11 [10]
NAT*: s=192.168.100.11->100.1.1.11, d=10.1.1.11 [9]
NAT: s=10.1.1.11, d=100.1.1.11->192.168.100.11 [11]
NAT*: s=192.168.100.11->100.1.1.11, d=10.1.1.11 [10]
NAT: s=10.1.1.11, d=100.1.1.11->192.168.100.11 [12]
NAT*: s=192.168.100.11->100.1.1.11, d=10.1.1.11 [11]

Router#no debug ip nat
IP NAT debugging is off
Router#show ip nat translations

```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	100.1.1.100:10	192.168.10.3:10	202.204.100.2:10	202.204.100.2:10
icmp	100.1.1.100:11	192.168.10.3:11	202.204.100.2:11	202.204.100.2:11
icmp	100.1.1.100:12	192.168.10.3:12	202.204.100.2:12	202.204.100.2:12
icmp	100.1.1.100:9	192.168.10.3:9	202.204.100.2:9	202.204.100.2:9
---	100.1.1.11	192.168.100.11	---	---

Router#

图 18 动态 NAT 配置

### 3.5.4 DNS 服务器配置测试

在校园网内主机 PC0 上打开浏览器，通过域名访问 Web 服务器，成功验证配置。

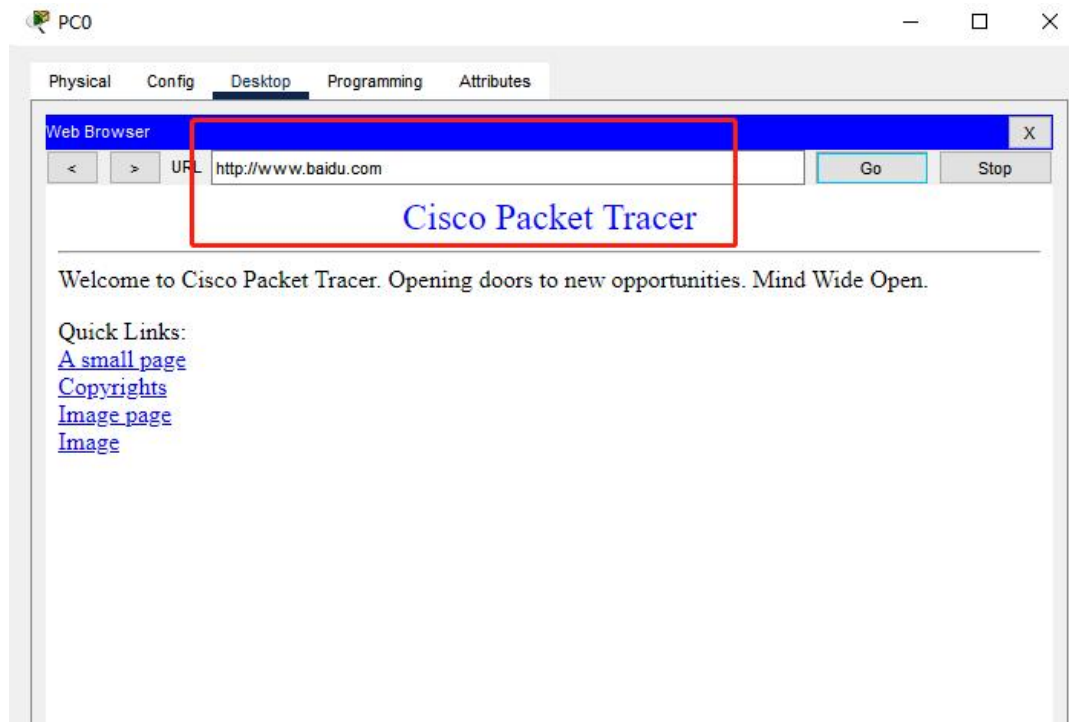


图 19 通过域名“www.baidu.com”访问 Web 服务器

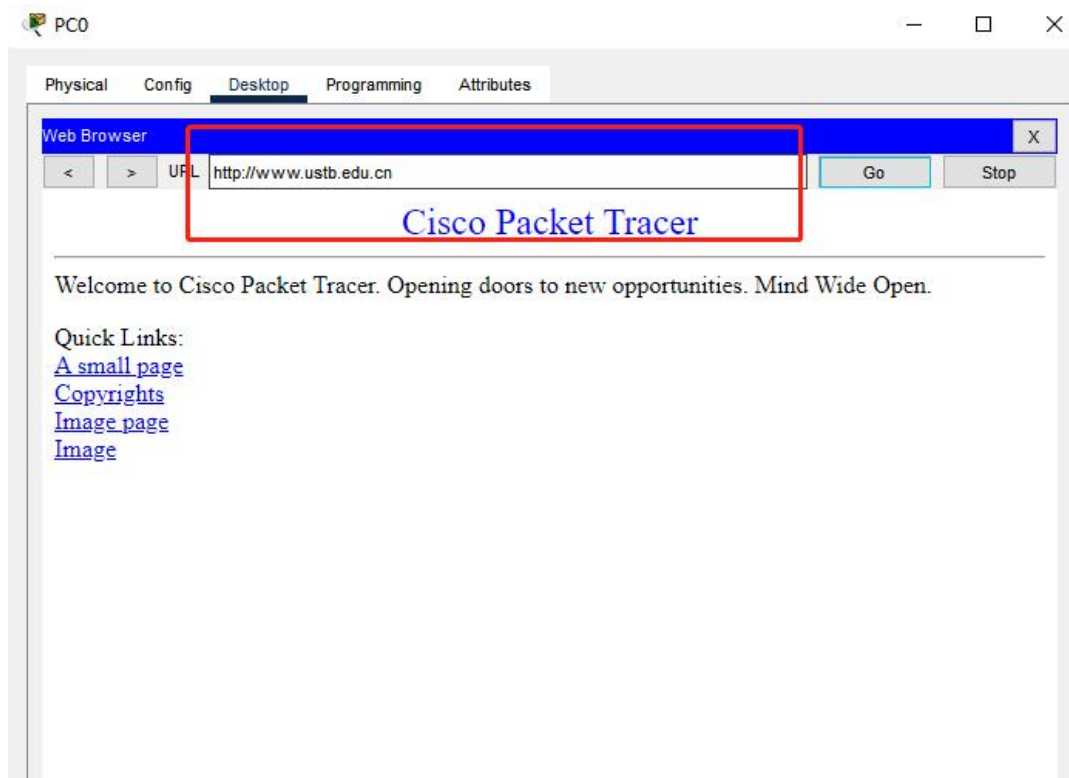


图 20 通过域名“www.ustb.edu.cn”访问 Web 服务器

### 3.5.5 FTP 服务器配置测试

在校园网内主机 PC0 上利用 FTP 服务器的 IP 地址使用 FTP 服务，通过命令“FTP 192.168.100.33”实现，使用管理员账号登入，进入后通过“dir”查看所有文件。成功验证配置。

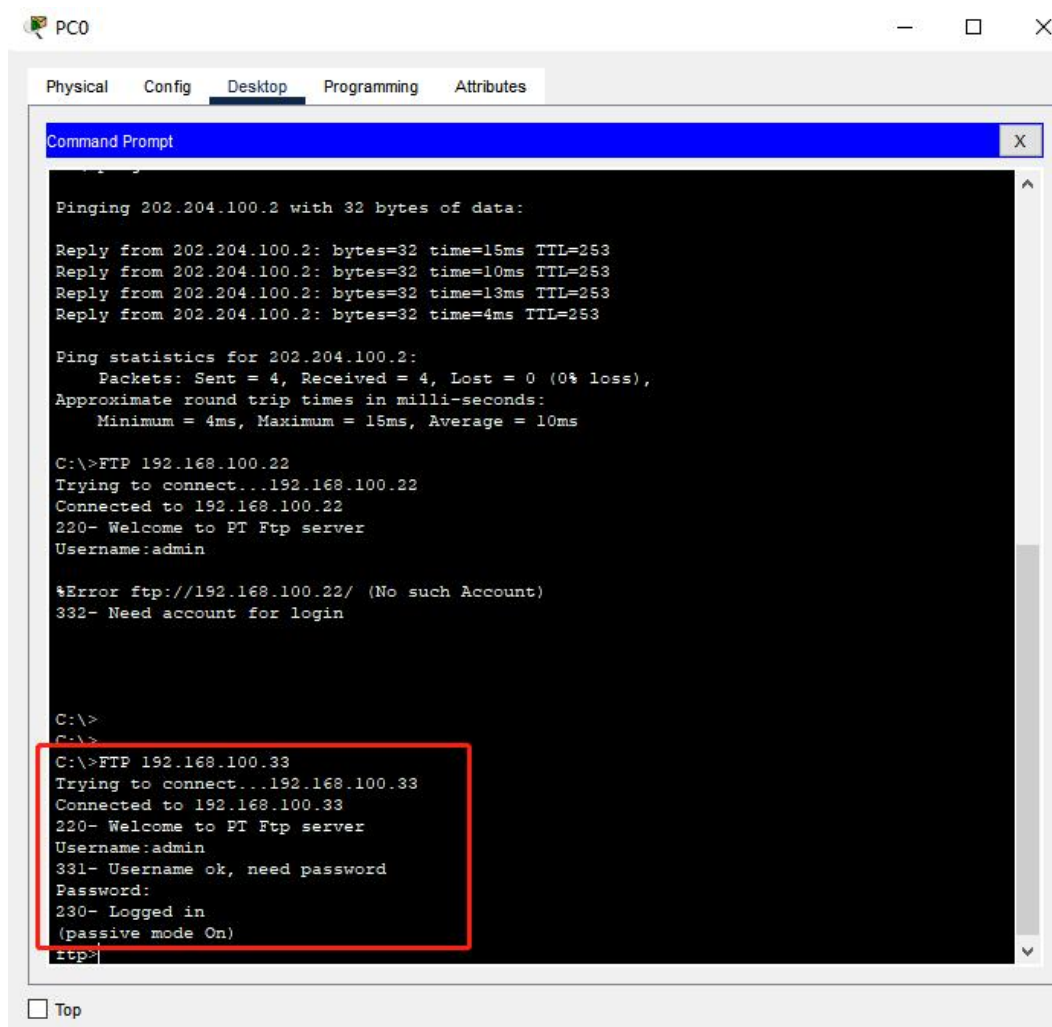
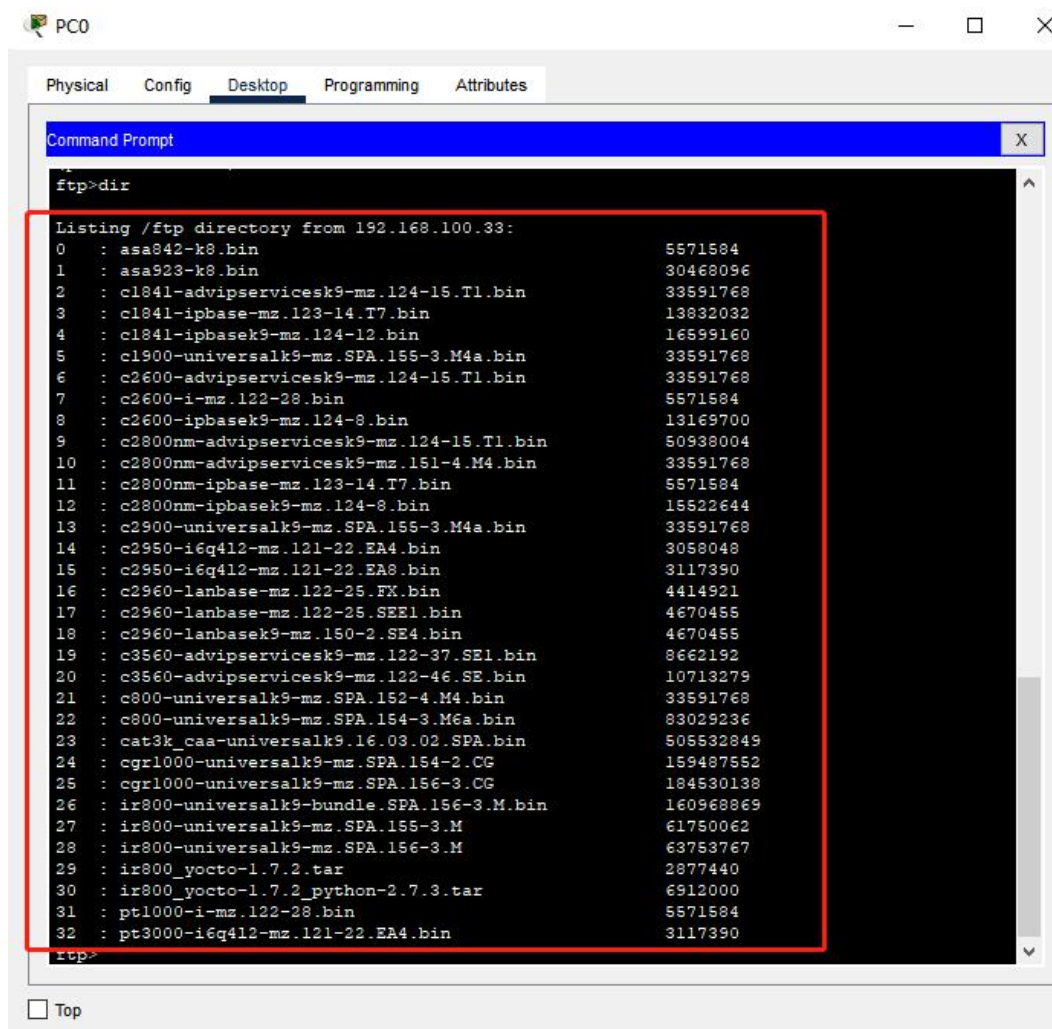


图 21 PC0 成功以管理员身份登入 FTP 服务器



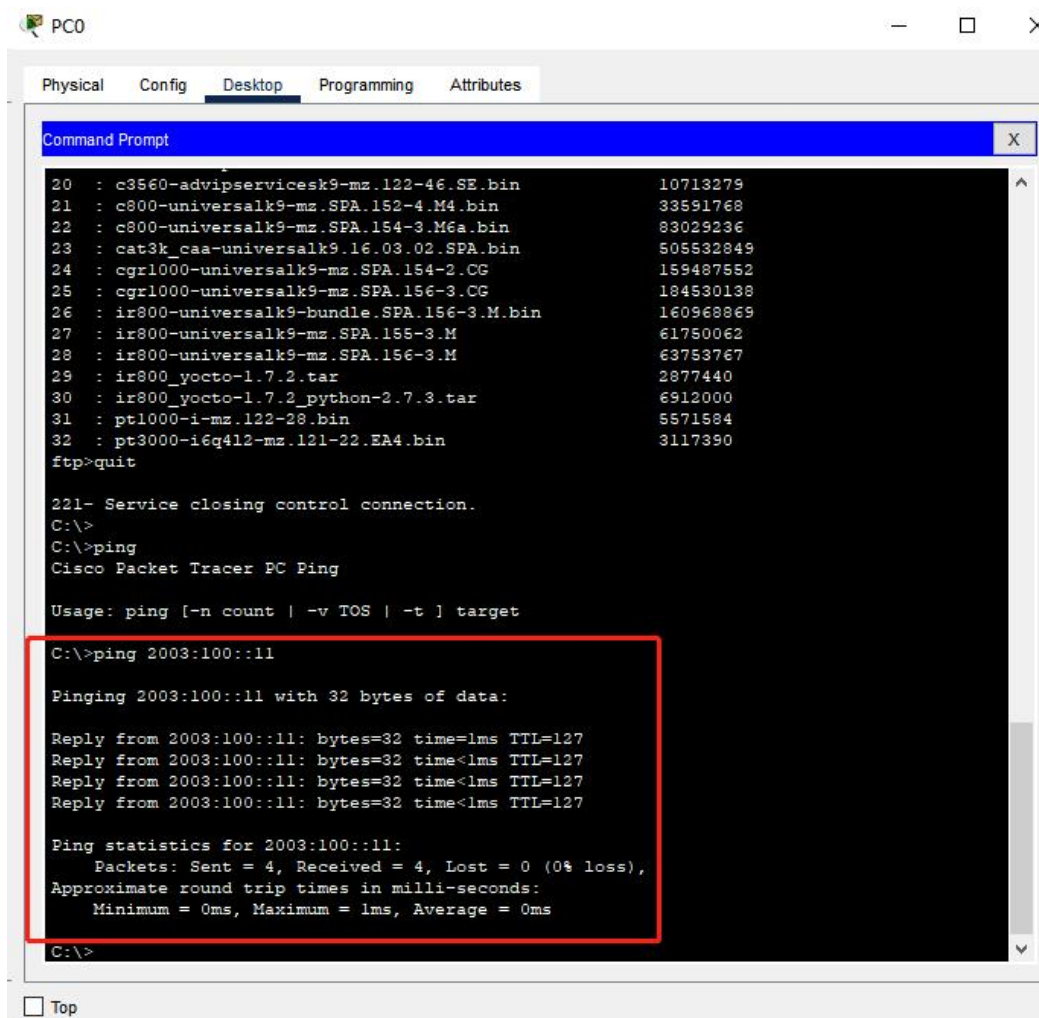
```
PCO
Physical Config Desktop Programming Attributes
Command Prompt
ftp>dir
Listing /ftp directory from 192.168.100.33:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M 61750062
28 : ir800-universalk9-mz.SPA.156-3.M 63753767
29 : ir800_yocto-1.7.2.tar 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-i-mz.122-28.bin 5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>
```

图 22 通过“dir”查看文件

### 3.5.6 IPv6 配置测试

本项目实现在校园网内部同时启用 IPv4 与 IPv6，下面针对 IPv6 配置进行测试：（1）校园网内部主机与数据中心的服务器的连通性；（2）校园网内部主机之间的连通性。经测试，成功验证 IPv6 配置。





The screenshot shows a window titled "PC0" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows a list of files with their sizes, followed by the command "ftp>quit". Below this, it shows "221- Service closing control connection." and "C:\>". The user then enters "C:\>ping" and "Cisco Packet Tracer PC Ping". The usage for ping is shown: "Usage: ping [-n count | -v TOS | -t ] target". The user then enters "C:\>ping 2003:100::11". The output shows the ping results for 2003:100::11, indicating successful connectivity with 0% loss.

```
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M 61750062
28 : ir800-universalk9-mz.SPA.156-3.M 63753767
29 : ir800_yocto-1.7.2.tar 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-i-mz.122-28.bin 5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>quit

221- Service closing control connection.
C:\>
C:\>ping
Cisco Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

C:\>ping 2003:100::11

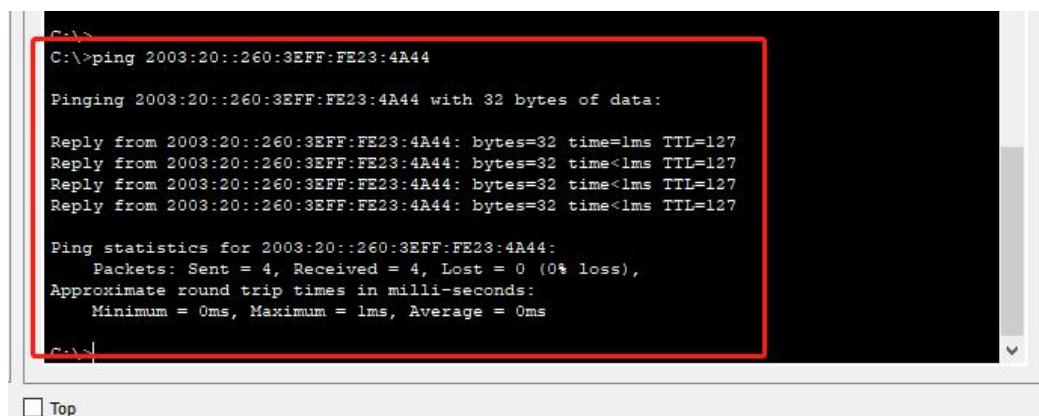
Pinging 2003:100::11 with 32 bytes of data:

Reply from 2003:100::11: bytes=32 time=1ms TTL=127
Reply from 2003:100::11: bytes=32 time<1ms TTL=127
Reply from 2003:100::11: bytes=32 time<1ms TTL=127
Reply from 2003:100::11: bytes=32 time<1ms TTL=127

Ping statistics for 2003:100::11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

图 23 主机与服务器的连通性测试



The screenshot shows a window titled "PC0" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The user enters "C:\>ping 2003:20::260:3EFF:FE23:4A44". The output shows the ping results for 2003:20::260:3EFF:FE23:4A44, indicating successful connectivity with 0% loss.

```
C:\>
C:\>ping 2003:20::260:3EFF:FE23:4A44

Pinging 2003:20::260:3EFF:FE23:4A44 with 32 bytes of data:

Reply from 2003:20::260:3EFF:FE23:4A44: bytes=32 time=1ms TTL=127
Reply from 2003:20::260:3EFF:FE23:4A44: bytes=32 time<1ms TTL=127
Reply from 2003:20::260:3EFF:FE23:4A44: bytes=32 time<1ms TTL=127
Reply from 2003:20::260:3EFF:FE23:4A44: bytes=32 time<1ms TTL=127

Ping statistics for 2003:20::260:3EFF:FE23:4A44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

图 24 主机与主机的连通性测试



## 二、总结与收获

### 1. 项目总结

通过在思科模拟器上进行校园网设计，我成功构建了一个包含教学区、学生公寓、计通学院和数据中心的多部门网络。这个设计不仅模拟了实际校园网络的结构，还考虑了不同部门的主机配置和服务需求。

在教学区、学生公寓和计通学院下配置的主机以及数据中心的服务器，为整个校园网络提供了丰富的测试场景。这样的设置有助于验证网络的可靠性和性能，确保各个部门能够顺畅地进行通信和服务访问。

通过在三层交换机上配置 DHCP 服务，我实现了教学区、学生公寓和计通学院内部设备的自动 IP 地址分配。这提高了网络管理的效率，减轻了手动配置的负担。

DNS 服务器的设置为校园网内部提供了域名服务，使得主机可以通过域名访问内部的 Web 服务器。这提升了用户体验，使网络资源更易于访问和管理。

FTP 服务器的配置为校园网内部提供了文件下载服务，为学生和教职员工提供了方便的文件共享和获取机制，增强了网络的实用性。

通过在 IPv4 基础上配置 IPv6 相关信息，我成功实现了整个校园网内部同时使用 IPv4 和 IPv6 地址。这有助于适应未来 IPv6 的普及，使网络更具扩展性和未来准备性。

在出口路由器上配置静态 NAT 和动态 NAT，成功实现了内部 WEB 服务器对外部主机的访问以及内部主机对互联网的访问。这为网络提供了安全而高效的连接，确保了内外通信的顺畅进行。

然而我的项目虽然满足了通用要求，但还存在部分问题，如未配置防火墙，未实现 DNS 域管理等。针对这些问题，会在后续的学习过程中逐步完善。

通过在思科模拟器上进行这一校园网设计，我深化了对网络拓扑设计、服务配置、IPv6 的理解，并提高了在实际网络环境中解决问题的能力。这样的实践经验对于今后从事网络工程和管理工作将是极为宝贵的。

### 2. 课程收获

在计算机网络实验课程的学习中，我获得了丰富的网络知识和实践经验，对计算机网络的原理、协议和技术有了更深入的理解。

(1) 理论与实践结合：通过实验，我成功将理论知识应用到实际场景中。从搭建简单的局域网

到设计复杂的校园网络，我深刻理解了计算机网络的各个层面，包括物理层、数据链路层、网络层、传输层和应用层等。

（2）网络拓扑设计与配置：在实验中，我学到了如何设计和配置网络拓扑。通过思考和规划，我成功创建了包括子网划分、VLAN 配置、路由设置等在内的多种网络场景。这为我在未来的实际工作中搭建和维护网络提供了宝贵的经验。

（3）IPv4 和 IPv6 共存：课程中的实验要求同时配置 IPv4 和 IPv6，使我深入了解了 IPv6 的特点和部署方式。这对于适应未来网络发展的趋势具有重要意义，为我具备了更广阔的网络视野。

（4）网络服务与安全配置：通过配置 DHCP、DNS、FTP 等服务，我学到了如何提供不同类型的网络服务。同时，通过实践网络安全策略、配置访问控制等，我增强了网络安全意识，为保护网络提供了基本技能。

（5）静态路由与动态路由：在实验中，我成功配置了静态路由和动态路由，了解了它们的优劣和适用场景。这对于构建更复杂网络、提高网络性能具有指导意义。

（6）NAT 技术的应用：课程中的实验涉及到 NAT 技术，我学到了如何配置静态 NAT 和动态 NAT，理解了 NAT 在解决 IPv4 地址短缺和提供网络安全性方面的重要作用。

（7）思科模拟器的应用：通过使用思科模拟器，我获得了实验环境的搭建和配置经验。这种虚拟化环境使我能够在安全的情况下进行实验，加深了对网络设备的操作和管理的理解。

计算机网络实验课程为我提供了一个全面而深入的网络学习平台。通过理论学习和实际操作相结合，我不仅增加了专业技能，而且培养了解决网络问题的能力，为未来在网络领域的职业发展奠定了坚实的基础。