湖南电子科技职业学院
HUNAN VOCATIONAL COLLEGE OF ELECTRONIC AND TECHNOLOGY

产品设计	方案设计	工艺设计
	√	

信息工程学院

毕 业 设 计

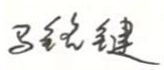
题目：湖鑫科技有限公司网络规划与设计

学生姓名	马铭键
学生学号	010425171787
班级名称	G32208 班
专业名称	计算机网络技术
指导教师	龙佳

2025 年 05 月

毕业设计真实性承诺及指导教师声明

本人郑重声明：所提交的毕业设计是本人在指导教师的指导下，独立进行研究工作所取得的成果，内容真实可靠，不存在抄袭、造假等学术不端行为。除毕业设计中已经注明引用的内容外，本设计不含其他个人或集体已经发表或撰写过的研究成果。对本毕业设计的研究做出重要贡献的个人和集体，均已在本设计中以明确方式标明。如被发现设计中存在抄袭、造假等学术不端行为，本人愿承担相应的法律责任和一切后果。

学生（签名）：  日　期：2025.5.11

指导教师关于学生毕业设计真实性审核的声明

本人郑重声明：已经对学生毕业设计所涉及的内容进行严格审核，确定其成果均由学生在本人指导下取得，对他人成果的引用已经明确注明，不存在抄袭等学术不端行为。

指导教师（签名）：  日　期：2025.5.15

（注：本页学生和指导教师须亲笔签名。）

目录

一、需求分析

（一）总体需求

湖鑫科技有限公司是一家专注于网络游戏开发的小型科技企业，对网络的依赖程度较高。近期，公司计划进行扩张，将总部单独迁移至新的办公地点。由于总部与分部相隔较远，公司决定采用运营商服务来实现总部与分部之间的网络互通，而非铺设专线。公司对网络的核心需求包括：确保总部与分部的稳定连接，实现关键部门与普通部门之间的数据隔离，满足员工日常的上网需求，以及保障网络通信的安全性。在资金预算的限制下，公司租用了 4 层写字楼作为分公司办公场所，同时租用了 2 层写字楼供总部使用。

（二）设备性能需求

鉴于公司业务的特殊性，网络设备的性能至关重要。随着公司业务的持续增长，未来网络流量将显著增加，设备所承受的压力也会不断上升。因此，设备性能必须能够在未来 10 年内保持稳定运行，其 CPU 的计算能力需与业务需求相匹配，以确保用户获得最佳的上网体验，尽量在不依赖缩短收敛时间技术的情况下，将延迟等指标降至最低。

（三）信息节点需求

分公司主要划分为三个区域：财务室、WLAN 区域和员工办公室。财务室的信息节点规划为 10 个，员工办公室的信息节点为 300 个，WLAN 区域则为员工和访客提供无线上网服务，规划了 350 个信息节点。总部主要服务于公司管理层和股东，信息节点规划为 30 个。此外，考虑到监控设备、打印机等哑终端的需求，总部额外增加了 10 个信息节点，分公司增加了 30 个信息节点。综上所述，公司总共规划了 730 个信息节点，其中总部 40 个，分公司 690 个。

二、总体规划

（一）方案设计

根据湖鑫科技有限公司的业务特性及未来几年网络发展趋势，随着流量数据的持续增长和公司规模的可能扩张，网络拓扑规划必须综合考虑以下关键要素：

（1）连通性

网络的基本功能是确保终端设备能够稳定上网，网络连接不能中断。出口设备需能高效转发内网流量至公网（运营商），满足日常上网需求。

（2）实用性

网络规划应贴合公司实际需求，追求性能与成本的平衡，为用户提供优质的上网体验。同时，为应对潜在故障，可采用 MSTP（多生成树协议）、ETH-TRUNK（链路聚合技术）或设备冗余等措施，提升网络的可靠性和稳定性。

（3）安全性

信息安全至关重要，数据泄露可能给公司带来巨大损失。近年来，使用国产设备和操作系统（如华为鸿蒙系统）成为保障信息安全的重要手段。公司需从内外两方面加强数据保护：对外，利用防火墙设备实施策略防护；对内，通过业务隔离和安全策略，防止内部人员访问关键部门主机窃取信息。

（二）网络拓扑规划

湖鑫科技有限公司的总部与分部网络拓扑规划如下。

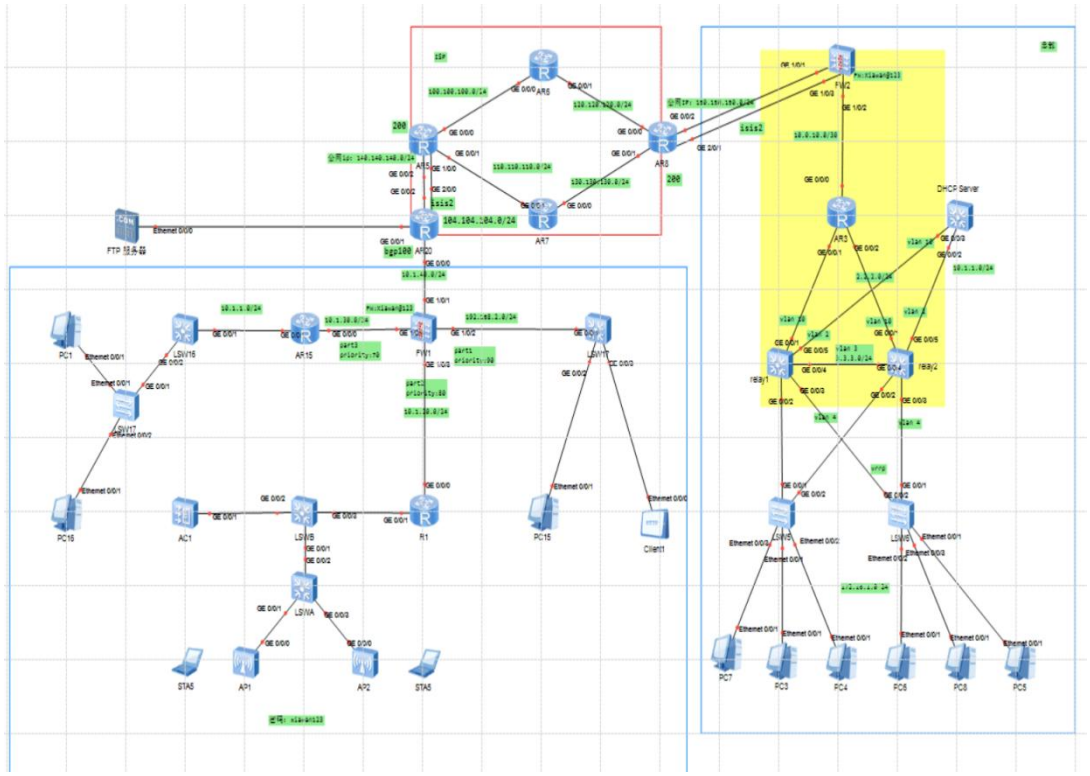


图 2.1 网络拓扑规划图

（1）总部拓扑规划

总部信息节点较少，且出于成本考虑，不部署 WLAN。所有设备通过 DHCP 分配 IP 地址，但为保障安全，需部署一台防火墙作为出口设备。

接入层：部署两台接入交换机，用于连接各办公室的 PC 终端设备。

汇聚层：采用两台交换机，通过 VRRP（虚拟路由冗余协议）技术配置虚拟网关，避免单点故障导致网络中断。

核心层：配置一台路由器，负责将汇聚层的流量转发至出口防火墙。

（2）分部拓扑规划

分部的拓扑规划思路与总部类似，但由于信息节点较多，接入层简化为一台交换机。分部包含三个独立区域，拓扑规划按区域划分。

财务室部分：信息节点较少，使用一台交换机作为接入设备，一台三层交换机作为汇聚设备，同时三层设备作为 DHCP 服务器。

（三）网络技术选型

（1）生成树协议（STP）

生成树协议（STP）主要用于接入层和汇聚层交换机之间，其核心功能是防止网络环路并提供链路冗余。STP 适用于所有厂商的设备，实现原理基本一致，因此被广泛应用。然而，STP 存在收敛速度较慢的缺点。为此，改进版本 RSTP 被提出，它解决了 STP 的大部分不足，并且能够兼容 STP 协议。但 RSTP 的局限性在于仅支持单棵“树”，无法实现流量负载分担。为解决这一问题，多生成树协议（MSTP）被定义。MSTP 继承了 STP 和 RSTP 的功能，兼容前两个版本，并且可以支持多棵“树”同时存在，提高了网络的冗余性和负载分担能力。

（2）动态主机配置协议（DHCP）

动态主机配置协议（DHCP）是一种让设备动态获取网络参数的协议。其产生的主要原因是手动配置网络参数存在诸多问题，如灵活性差、容易出错、利用率低以及管理员工作量大。DHCP 的主要优点包括灵活方便、效率高以及管理便捷。

（3）开放式最短路径优先（OSPF）

开放式最短路径优先（OSPF）是一种基于链路状态的动态路由协议，用于与使用相同协议的设备建立邻居和邻接关系，实现网络互通。OSPF 是一种内部网关协议（IGP），目前有两个版本：版本 2 适用于 IPv4，版本 3 适用于 IPv6。OSPF 主要应用于网络的核心层和汇聚层，通过 SPF 算法实现优化传输，广泛应用于中大型网络。

（4）双向转发检测（BFD）

双向转发检测（BFD）是一种通用的标准故障检测机制，与传输介质和协议无关。其主要作用是快速检测链路故障，最大的优点是采用单一机制对任何协议层进行实时监测。BFD 支持静态和动态两种建立方式，并有三种会话状态（down、init、up）。它可以与静态和动态路由协议联动，实现毫秒级故障检测。

（5）虚拟路由冗余协议（VRRP）

虚拟路由冗余协议（VRRP）旨在解决单网关的弊端并提高网络可靠性。VRRP 可以将两台物理设备逻辑合成一台设备，使用同一个网关地址，既解决了多网关的不便，又避免了单网关设备可能造成的单点故障。VRRP 部署在接口上，需要进行主备选举、切换和回切。此外，VRRP 还可以实现负载分担，并与 BFD 和 MSTP 等技术或协议联动使用。

（四）备选型

根据公司对网络规划的资金投入，经过对市场主流网络设备的多方面对比，最终选择了华为的路由器、交换机、防火墙和服务器等设备。设备的具体参数如下：

（1）接入交换机：

接入层交换机需要有足够的端口接入主机，并且对 CPU 的计算处理能力要求较高。公司选择了华为 S3700 系列交换机，其参数如图 2.2 所示。

产品名称	华为 S3700-28TP-SI-AC
上行端口速率	千兆
下行端口速率	百兆
产品单价	￥2295
端口数量	24 口
端口类型	电口&光口
散热方式	风扇散热
源产地	中国大陆
适用网络	中小型网络
网管类型	网管
端口供电功能	非 POE 供电
适用场景	汇聚交换机

图 2.2 S3700-28TP-SI-AC 主要参数

（2）核心交换机：

核心交换机作为网络拓扑的关键节点，处于“承上启下”的核心位置，对性能要求极高。经过对市场主流产品的对比分析，公司选择了华为的核心交换机。该设备基于华为自主研发的 VRP 平台，具备市场上同类产品的功能，并支持多种应用场景。具体参数如图 2.3 所示。

产品名称	华为 S5700S-L32ST4X-A1
上行端口速率	万兆
下行端口速率	千兆
产品单价	￥5500
端口数量	24 口
端口类型	光口
散热方式	风扇散热
源产地	中国大陆
适用网络	中大型网络

图 2.3 华为 S5700S-L32ST4X-A1 主要参数

（3）防火墙：

防火墙设备选用了华为 USG6000E 系列中的 USG6309E-AC 型号。该系列视频安全网关通过设备指纹认证、流量指纹认证以及入侵防御系统，构建了摄像机安全接入的三重防线，有效保障了摄像机的安全接入。该产品的详细参数如图 2.4 所示。

产品名称	华为 USG6309E-AC
类型	有线路由器
企业 VPN	支持
产品单价	￥14999
LAN 输出口	千兆网口
WAN 接入口	千兆网口
支持 IPV6	支持
LAN、WAN 口类型	光口，电口
防火墙	支持
AP 管理	不支持

图 2.4 华为 USG6309E-AC 主要参数

（4）路由器：

根据公司的网络拓扑规划和资金预算，路由器设备均选用了华为 AR6000 系列产品。该系列产品在性能、功能和可靠性方面均能满足公司网络拓扑的需求。具体参数如图 2.5 所示。

产品名称	华为 AR6280-S
类型	有线路由器
企业 VPN	支持
产品单价	￥10999
LAN 输出口	千兆网口
WAN 接入口	千兆网口
支持 IPV6	支持
LAN、WAN 口类型	光口，电口
防火墙	支持

图 2.5 AR6280-S 主要参数

（5）AP：

无线接入点（AP）的功能是为移动终端提供无线上网服务，类似于家用路由器。为满足公司大量员工的无线上网需求，公司选用了华为 AP4050DN-E 产品。该产品整机速率高达 1.267Gbps，适合部署在商场、超市、医院和学校等场景。具体参数如图 2.6 所示。

产品名称	华为 AAP4050DN-E
电源输入	POE/DC
天线类型	内置天线
总带机数	50-100
LAN 口类型	电口
支持 IPV6	支持
无线协议	Wi-Fi 5

图 2.6 AP4050DN-E 主要参数

（6）AC：

无线接入控制器的功能是管理和控制 AP 设备以及转发数据。公司选用了华为 AC6000 系列产品，该产品具备高度的灵活性，能够适应多种应用场景。具体参数如图 2.7 所示。

产品名称	华为 AC6800V
端口	6 x GE + 6 x 10 GE
电源	AC
转发能力	60Gbit/s
最大可管理 AP 的数量	10240
最大可接入用户数	102400

图 2.7 AC6800V 主要参数

三、项目实施

（一）公司总部

根据总部的信息节点需求和拓扑规划，总部终端设备通过 DHCP 动态分配 IP 地址。由于总部无需考虑隔离需求，所有终端设备统一使用 172.16.1.0/24 网段。在 DHCP 服务器上配置地址池，核心交换机通过 VRRP 作为 DHCP 中继，提升网络稳定性。为防止物理链路故障导致网络中断，采用 BFD 技术快速检测链路状态。总部内网使用 OSPF 协议实现全网互联互通，出口防火墙配置信任区域（内网）和非信任区域（外网），通过 NAT 技术中的 Easy IP 进行地址转换。

（二）公司分部

根据分部的信息节点划分和业务隔离需求，分部网络采用防火墙进行隔离。

（1）员工办公室部分：

使用 DHCP 为员工主机分配网络参数，路由器 AR15 作为 DHCP 服务器，下游设备作为中继机，并采用 DHCP Snooping 技术增强安全性。

（2）WLAN 部分：

鉴于 WLAN 部分信息节点多、管理难度大，采用三层旁挂组网方式。AC 旁挂三层组网，减轻路由器工作负担，确保流量正常转发。DHCP 部署方式为 AC 为 AP 分配地址，路由器为终端（如 Sta）分配地址，采用直接转发方式传输流量。

（3）财务室部分：

财务室信息节点少且数据机密性高，终端用户 IP 地址及相关配置由管理员手动设置。

（4）服务器：

服务器连接至出口路由器，出口路由器上配置安全策略，仅允许内部流量访问服务器，阻止外网流量访问。

（5）防火墙：

防火墙作为安全设备，隔离所有流量。为保障内网用户访问服务器和外网，配置不同安全区域策略进行流量转发。鉴于设备特性，使用 OSPF 等动态路由协议较为复杂，且内部路由条目数量有限，因此采用静态路由实现内网用户与外网及服务器的互通。

（三）总、分公司间的互通

受地理位置限制，公司选择购买运营商服务，采用 MPLS VPN 实现总、分公司业务通信。运营商设备启用 MPLS，PE 设备间通过 MP-BGP 传递公司内部流量，PE 与 CE 通过动态路由协议交换路由信息，确保总、分公司通信顺畅。

（四）IP 地址、VLAN 规划

网络设计中，IP 地址和 VLAN 规划至关重要，不合理规划可能导致网络故障。同一设备或拓扑中不可存在重复 IP 地址，VLAN 接口下亦然，否则可能引发 ARP 欺骗等问题。严谨的 IP 地址和 VLAN 规划是网络稳定运行的基础。

（1）公司总部内网 IP 地址规划

路由器与防火墙间：10.0.10.0/30

路由器与核心交换机：1.1.1.0/24、2.2.2.0/24

DHCP 服务器与交换机：10.1.1.0/24

终端地址池：172.16.1.0/24

表 3.1 总部 IP 地址规划表

设备	端口	IP 地址	掩码
FW2	G1/0/1	150.150.150.1	255.255.255.0
	G1/0/2	10.0.10.1	255.255.255.252
AR3	G0/0/0	10.0.10.2	255.255.255.252
	G0/0/1	1.1.1.1	255.255.255.0
	G0/0/2	2.2.2.1	255.255.255.0
Relay1	Vlanif10	10.0.11.2	255.255.255.252
	Vlanif3	3.3.3.1	255.255.255.0
	Vlanif2	10.1.1.2	255.255.255.0
	Vlanif4	172.16.1.253	255.255.255.0
Relay2	Vlanif10	2.2.2.1	255.255.255.0
	Vlanif3	3.3.3.2	255.255.255.0
	Vlanif2	10.1.1.3	255.255.255.0
	Vlanif4	172.16.1.252	255.255.255.0
DHCP Server	Vlanif10	10.1.1.1	255.255.255.0

（2）公司总部内网 VLAN 及 IP 地址规划

LSW2 和 LSW3 上创建 4 个 VLAN，分别是：

Vlanif2：10.1.1.0/24

Vlanif3：3.3.3.0/24

Vlanif4：172.16.1.0/24

Vlanif10：1.1.1.0/24

表 3.2 总部 VLAN 规划表

设备	LAN 号	端口	IP 段
LSW2	VLAN 2	G0/0/5	10.1.1.0/24
	VLAN 3	G0/0/4	3.3.3.0/24
	VLAN 4	G0/0/3	172.16.1.0/24
	VLAN 10	G0/0/1	1.1.1.0/24
LSW3	VLAN 2	G0/0/5	10.1.1.0/24
	VLAN 3	G0/0/4	3.3.3.0/24
	VLAN 4	G0/0/3	172.16.1.0/24
	VLAN 10	G0/0/1	1.1.1.0/24
LSW7	VLAN 10	G0/0/2	10.1.1.0/24
		G0/0/3	10.1.1.0/24

（3）公司分部 IP 地址规划

防火墙与 AR20：10.1.40.0/24

防火墙与 AR15：10.1.30.0/24

防火墙与 R1：10.1.20.0/24

表 3.3 分部 IP 地址规划表

设备	端口	IP 地址	掩码
FW1	G1/0/1	10.1.40.1	255.255.255.0
	G1/0/3	10.1.20.1	255.255.255.0
	G1/0/4	10.1.30.1	255.255.255.0
AR20	G0/0/0	10.1.40.2	255.255.255.0

	G0/0/2	140.140.140.1	255.255.255.0
AR15	G0/0/0	10.1.30.2	255.255.255.0
R1	G0/0/0	10.1.20.2	255.255.255.0
	Vlanif102	10.23.102.2	255.255.255.0
FTP 服务器	E0/0/0	192.168.10.1	255.255.255.0

（4）公司分部 VLAN 和 IP 地址规划

公司分部的 VLAN 和 IP 地址规划详细信息如表 3.4 所示。在 LSW16 上创建了 VLAN10，其对应的网段为 10.1.1.0/24。对于 LSWB，规划了以下 VLAN 接口及其对应的网段：

Vlanif10：10.23.10.0/24

Vlanif100：10.23.100.0/24

Vlanif101：10.23.101.0/24

Vlanif102：10.23.102.0/24

表 3.4 分部 VLAN 规划表

设备	LAN 号	端口	IP 段
LSW16	VLAN 10	G0/0/1	10.1.1.0/24
LSWB	VLAN 10	G0/0/1	10.23.10.0/24
	VLAN 100	G0/0/2	10.23.100.2.0/24
	VLAN 101	G0/0/1	10.23.101.0/24
		G0/0/3	10.23.101.0/24
	VLAN 102	G0/0/1	10.23.102.0/24
		G0/0/3	10.23.102.0/24
AC1	VLAN 100	G0/0/1	10.23.100.0/24

四、网络实现

（一）服务器配置

FTP 服务器为公司提供文件存储与访问服务，对于以游戏开发为主营业务的公司而言，日常运营会产生大量文件，FTP 服务器能够有效满足这一需求。FTP 服务器的基本配置地址为 192.168.10.1，其网关设置在出口路由器上，网关地址为 192.168.10.254。服务器的具体配置如图 4.1 所示：

图 4.1 FTP 服务器基础配置

（二）核心交换机配置

核心交换机部分配置命令选取自公司总部设备，其主要功能包括实现 VRRP 热备份、DHCP 中继，通过 OSPF 协议保障内网互联互通，并结合 BFD 技术提升转发效率及物理链路状态检测能力。具体配置如下：

```
LSW2:
interface Vlanif4
 ip address 172.16.1.253 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.1.254
 vrrp vrid 1 priority 120
 vrrp vrid 1 track interface GigabitEthernet0/0/5 reduced 30
 ospf enable 1 area 0.0.0.1
 dhcp select relay
 dhcp relay server-ip 10.1.1.1
#
ospf 1 router-id 10.1.1.2
 bfd all-interfaces enable
 bfd all-interfaces min-tx-interval 100 min-rx-interval 100
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
```

（三）接入交换机配置

接入设备主要用于终端设备的接入，通常无需手动配置。然而，随着网络技术的发展和黑客攻击手段的日益复杂，为防止黑客通过接入设备随意接入非法设备，特配置DHCP Snooping 技术以隔绝非法 DHCP 服务器。具体配置如下：

```
dhcp enable
#
dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping trusted
```

（四）路由器配置

出口路由器的主要职责是执行 NAT（网络地址转换）。分部出口设备采用路由器，NAT 配置采用地址池方式。其余路由器设备仅进行了静态路由等基础配置。具体配置如下：

```
AR20:
acl number 2000
 rule 5 permit
#
 nat address-group 1 140.140.140.10 140.140.140.20
#
interface GigabitEthernet0/0/0
 ip address 10.1.40.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 192.168.10.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 140.140.140.1 255.255.255.0
 nat outbound 2000 address-group 1
#
ip route-static 10.1.0.0 255.255.0.0 10.1.40.1
ip route-static 10.23.101.0 255.255.255.0 10.1.40.1
ip route-static 10.23.102.0 255.255.255.0 10.1.40.1
ip route-static 192.168.1.0 255.255.255.0 10.1.40.1
ip route-static 192.168.2.0 255.255.255.0 10.1.40.1
```

（五）防火墙配置

公司分部防火墙用于隔离内网不同部分，定义了四个不同的安全区域，并将接口分配至相应区域，实现各分部流量隔离。同时，允许流量向上级设备路由，并根据公司内网要求配置相应安全策略。公司总部防火墙则作为出口设备，采用 easy-ip 进行 NAT 地址转换，将内网和外网接口分别加入 trust 区域和 untrust 区域。重要配置如下：

```
 add interface GigabitEthernet1/0/1
#
firewall zone name part1 id 6
 set priority 90
 add interface GigabitEthernet1/0/2
#
firewall zone name part2 id 7
 set priority 80
 add interface GigabitEthernet1/0/3
#
security-policy
 rule name part3_to_out
  source-zone part3
  destination-zone out
  action permit
 rule name part1_to_out
  source-zone part1
  destination-zone out
  action permit
 rule name part1_to_out
  source-zone part1
  destination-zone out
  source-address 192.168.2.0 mask 255.255.255.0
  action permit
 rule name part2_to_out
  source-zone part2
  destination-zone out
  action permit
```

（六）总分部联通主要配置

公司总部与分部之间的通信通过运营商的 MPLS VPN 技术实现，两端配置基本一

致。运营商的 PE 设备上配置相应的 VRF（虚拟路由转发实例），CE 设备与 PE 设备运行 ISIS 协议，通过引入内网路由实现总部与分部之间的通信。

```
ip vpn-instance VPN_B
 ipv4-family
  route-distinguisher 100:200
  vpn-target 100:200 export-extcommunity
  vpn-target 200:100 import-extcommunity
#
mpls lsr-id 150.1.5.5
mpls
#
mpls ldp
 #
bgp 200
 peer 150.1.8.8 as-number 200
 peer 150.1.8.8 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 150.1.8.8 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 150.1.8.8 enable
 #
 ipv4-family vpn-instance VPN_B
  import-route isis 2

isis 2
 network-entity 49.0001.0000.0000.0020.00
 import-route static
 import-route ospf 1
#
ospf 1
 import-route isis 2
 area 0.0.0.0
  network 10.1.40.0 0.0.0.255
```

五、网络测试

（一）员工上网测试

公司内部终端设备需满足能够访问外网，但禁止访问财务室主机的要求。财务室的测试终端使用 IP 地址 192.168.2.1，而员工办公室的测试终端使用 IP 地址 192.168.1.253。为直观展示测试效果，采用 Ping 测试进行验证。财务室与其他部分的不连通性测试结果如图 5.1 所示：

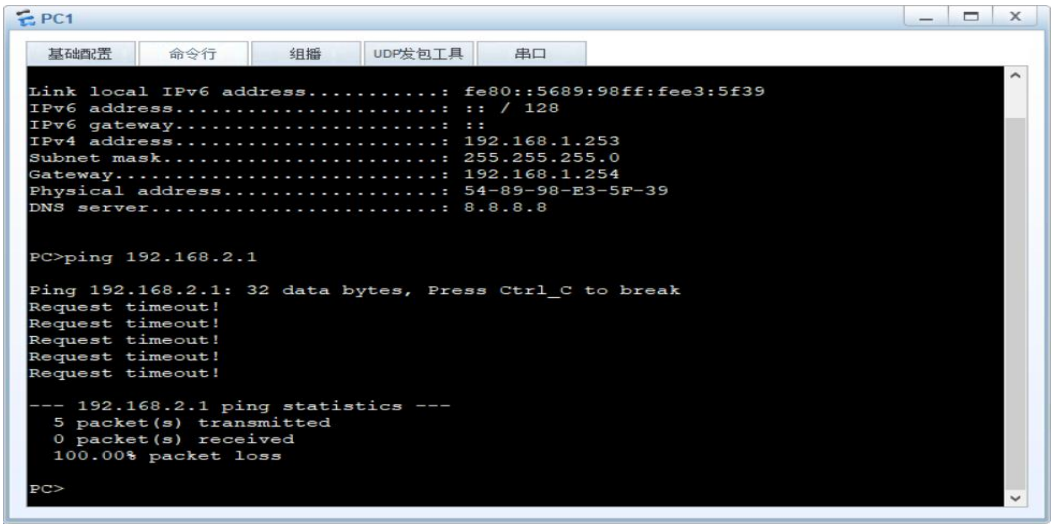


图 5.1 内网终端不互通测试

外网连通性测试通过公司分部员工办公室的主机进行，该主机通过 DHCP 获取的 IP 地址为 192.168.1.253，目标为运营商的 IP 地址 140.140.140.2。外网连通性测试结果如图 5.2 所示：

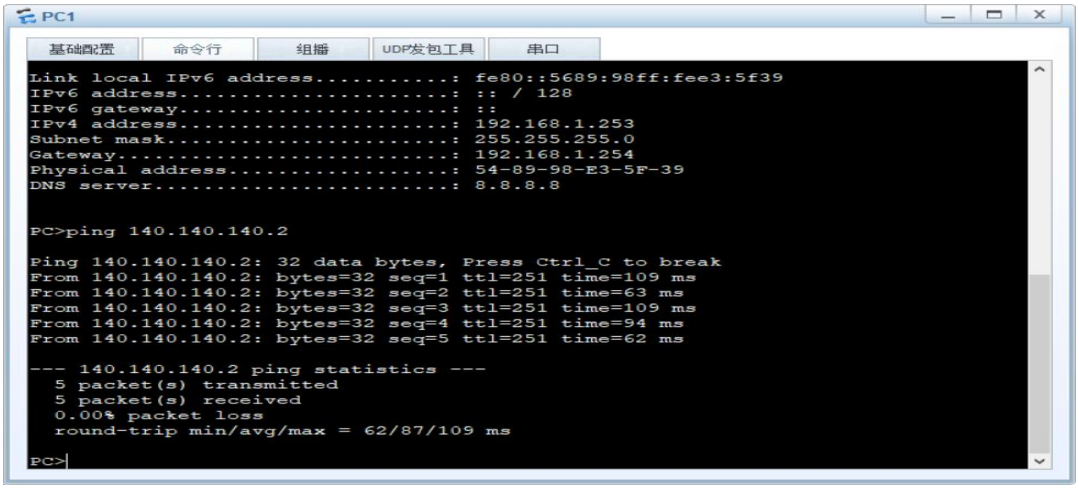


图 5.2 外网连通测试

（二）服务器测试

FTP 服务器的测试通过客户机完成，包括登录服务器、从服务器下载文件以及向服务器上传文件。在华为 eNSP 模拟器中，登录成功后页面将显示本地和服务器的文件列表。文件上传和下载成功时，系统会弹出提示框显示操作成功。FTP 服务器登录测试页面如图 5.3 所示。

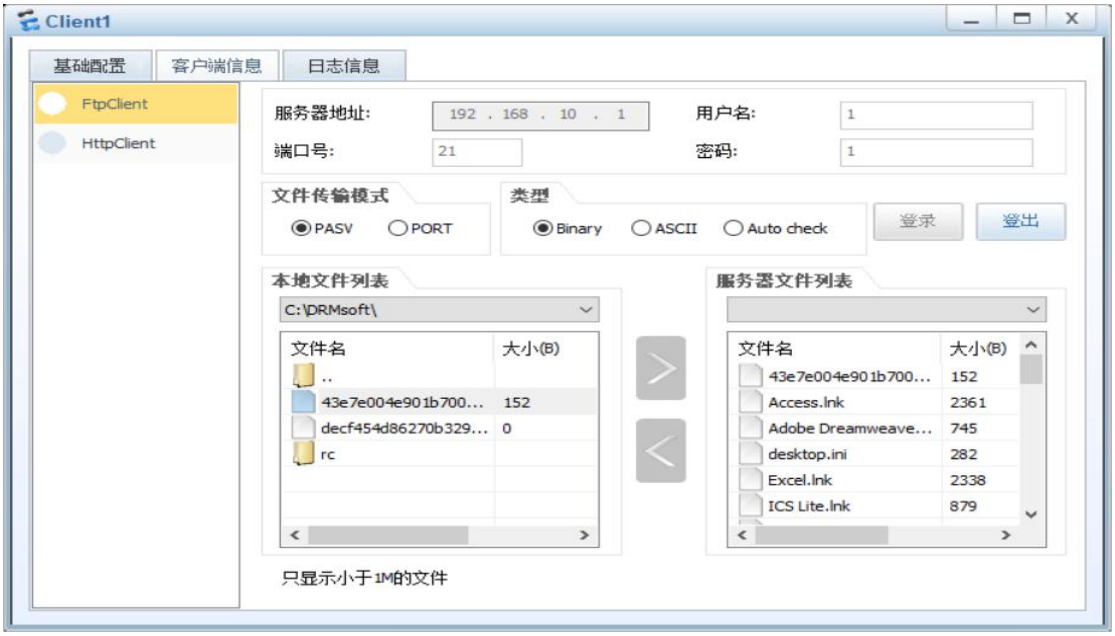


图 5.3 登录成功页

文件上传测试页面如图 5.4 所示：

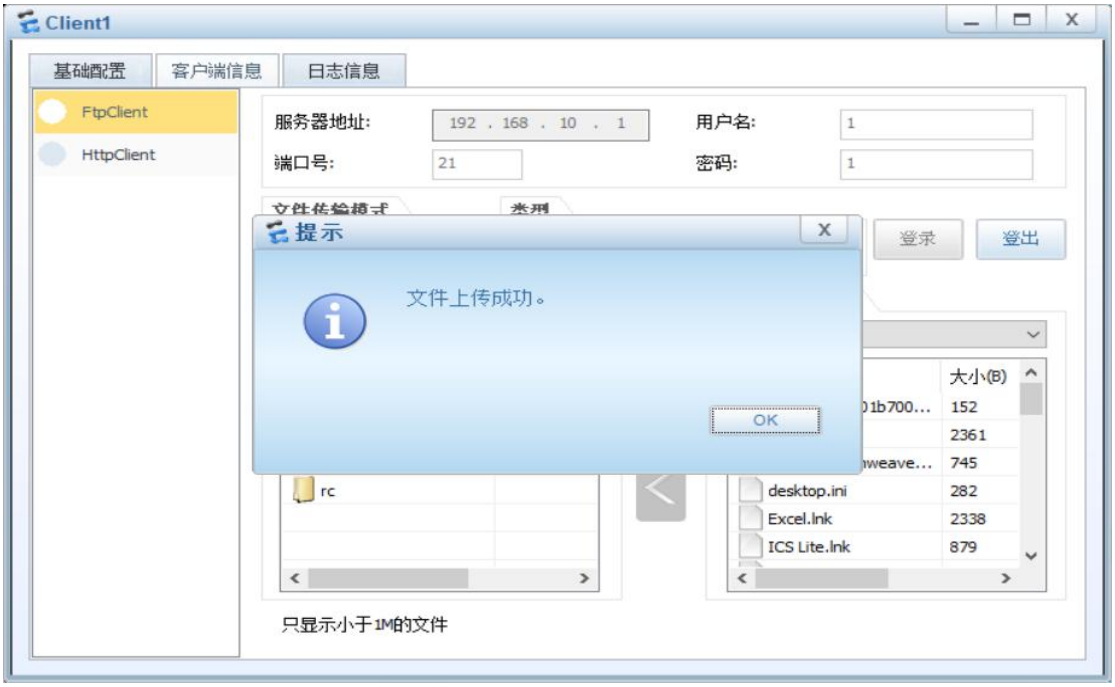


图 5.4 上传成功页

文件下载测试页面如图 5.5 所示：

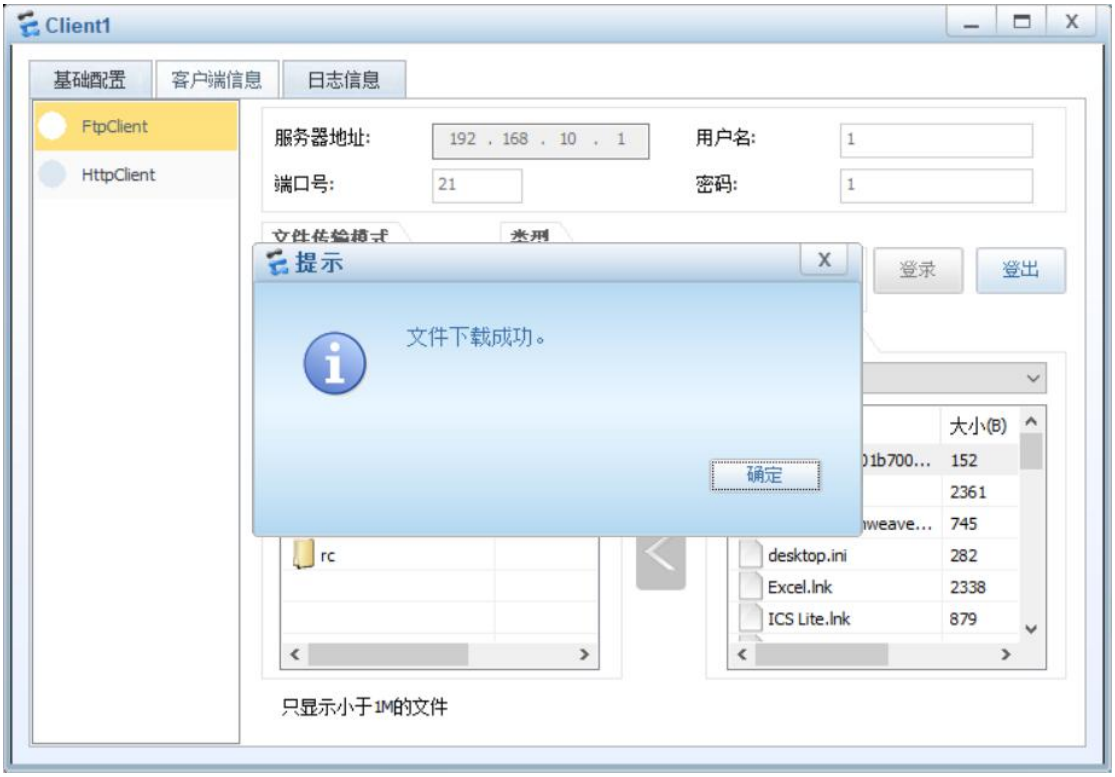


图 5.5 下载成功页

（三）公司总分部通信测试

总部与分部员工办公室联通测试如图 5.6 所示：

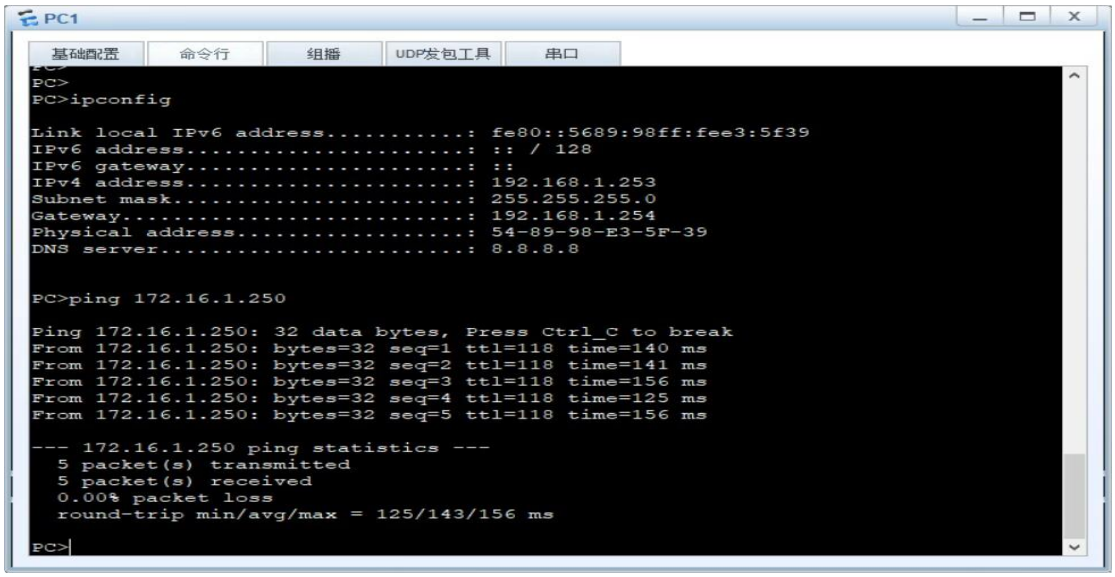


图 5.6 总分测试成功页

总部与分部无线联通测试入图 5.7 所示：

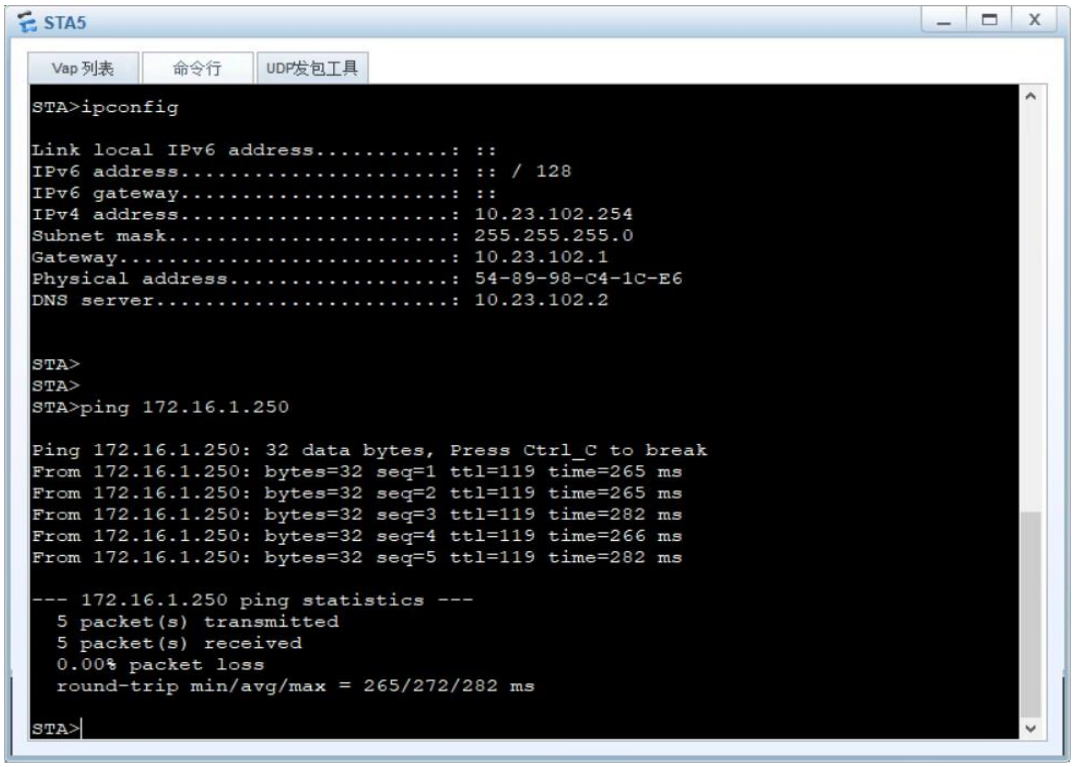


图 5.7 总部与分部无线测试成功页

参考资料

[1] 何朝阳，欧玉芳，曹祁．美国大学翻转课堂教学模式的启示[J]．高等工程教育研究，2024(3)．

[2] 刘彬让．研究型农业大学本科人才培养体系的构建[J]．高等农业教育，2023(11)．

[3] 刘彬让，李论．试论研究型农业大学教学方法的改革[J]．高等农业教育，2024(7)．

[4] 张利荣．我国本科生学习现状的调查与分析——以武汉地区高校为例[J]．国家教育行政学院学报，2022(4)．

[5] 杨俊，王光明，张玘．影响本科研究型教学实施效果的教师因素分析[J]．高等教育研究(成都)，2024(4)．

[6] 黄小兵，王海燕，周诗彪，等．地方高校应用化学本科毕业论文改革探索[J]．广州化工，2023，41(20)：158-159．

[7] 毛姣艳．翻转课堂教学模式的优势与应用挑战[J]．时代教育，2024(7)．

[8] 赵兴龙．翻转教学的先进性与局限性[J]．中国教育学刊，2023(4)．

[9] 乌文波．中职学校校园网络的规划与设计[J]．数码设计，2023，18(07)：173-174．

[10] 陈岳．园区级校园网络规划与方案设计[J]．信息技术与信息化，2024(11)：167-170．