



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： 胜天公司网络规划与设计方案

学生姓名 唐鹏

学生学号 010425171786

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）：唐鹏 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）：尤佳 日期：2025.5.16

（注：本页学生和指导教师须亲笔签名。）

目 录

一、需求分析	1
(一) 总体需求	1
(二) 性能需求	1
(三) 信息节点需求	2
二、胜天公司网络总体规划	4
(一) 方案设计原则	4
(二) 总体设计	4
1. 分层网络设计	4
2. 胜天公司网拓扑结构	5
(三) 网络技术选型	6
1. 网络设备选型	7
2. 网络抗干扰性	7
三、胜天公司网络工程建设	9
四、网络实现	14
(一) 服务器配置	14
(二) 核心交换机配置	15
(三) 二层交换机配置	16
(四) 出口防火墙配置	17
(五) ISP 路由器配置	18
五、网络测试	19
(一) 物理网络连通测试	19
(二) 无线网络连通性测试	21
(三) AP 上线测试	21
(四) 服务器网测试	22
六、总 结	25
参考资料	27

一、需求分析

(一) 总体需求

胜天公司原为一家员工人数不超过 200 人的小型企业。凭借“诚信为本”的经营理念，公司赢得了客户的广泛认可，进而获得了大客户的注资与扩建机会。此次扩建包括对公司网络布局的重新规划与部署。根据公司要求，网络需划分为多个独立区域，分别服务于销售部、财务部、保安部、人事部、市场部、办公大厅一楼、办公大厅二楼及总裁办公室。网络中心机房则依据公司要求及实际情况，部署于办公大厅二楼的中心位置。

公司各部门需能正常访问网络，但出于安全考虑，财务部与总裁办公室的网络访问权限受到限制，其他部门无法访问这两个部门的网络。部分业务需访问外部服务器，而部分业务则仅限于访问内部服务器。为满足这一需求，公司采用 DNS 地址切换策略：访问内部服务器时使用内部 DNS，访问外部服务器时则切换至外部 DNS。

为确保业务流量安全、网络故障快速恢复以及应对突发业务需求，公司网络采用接入层、汇聚层、核心层的三层体系结构。核心层部署防火墙，防范外网非法入侵，保障内网安全；汇聚层则配备两台高性能交换机，一台为主设备，另一台为备用设备，一旦主设备出现故障，备用设备将自动切换为主设备，确保业务连续性。

(二) 性能需求

胜天公司网络需满足以下性能需求：

- (1) 提供快速的互联网接入，支持 FTP、HTTP、DNS 等互联网服务。
- (2) 各部门电脑通过接入交换机实现互访，促进资源共享。
- (3) 出口部署防火墙，划分不同安全区域，最大化保障内网安全。
- (4) 网络拓扑具备可扩展性和健壮性，便于未来业务增长时快速部署机房设备。
- (5) 在保障网络安全的前提下，工程师需每周定期检查网络环境，更新病毒库和防火墙。
- (6) 通过将不同部门划分至不同 VLAN，减少广播流量，避免带宽浪费，提升

网络访问安全性。

(7) 安保部门采用千兆链路，业务部采用万兆链路，满足各部门需求。

(8) 部署 ACL 等策略，限制某些部门间的访问，进一步提高内部网络访问安全性。

(9) 部署内部服务器，满足员工快速访问和资源共享需求，实现网络互访。

(三) 信息节点需求

(1) 保安部及各保安亭、摄像头共需 30 个信息节点。

(2) 办公大厅共两层（1F、2F），包含 40 间办公室、2 个大厅、每层各 1 间会议室，二楼设有弱电间。根据各办公室人数和业务需求，每间办公室设置 1 个信息节点，会议室各设置 2 个信息节点，大厅各设置 2 个信息节点。此外，每层大厅各设置 2 个无线 AP，方便客户接入，共计 55 个信息节点。

(3) 市场部、销售部、人事部、财务部、总裁办公室分布在 3F 至 6F 共四层，共有 80 间办公室、4 个会议室。根据办公性质和人数，每间办公室设置 1 个信息节点。为便于管理，每层每部门各设 1 个弱电间。财务部与总裁办公室因业务需求需互相访问，共计 84 个信息节点。

各个部门信息节点数量如表 1.1 所示：

表 1.1 信息节点对应数量

项目名称	部门	设备名称	设备型号	接口数量	数量	楼层名称	楼层总数	总节点数
胜天公司	安保部	交换机	S3700	24	2	1F	6	169
		摄像头	DS-IPC-B13HV2-IA	1	30			
	办公大厅	交换机	S3700	24	2	1F、2F		
		<u>M-AP</u>	RJ-AP480	4	44			
		<u>G-AP</u>	RJ-AP850	1	2			
	市场部	交换机	S3700	24	1	3F		
		<u>M-AP</u>	RJ-AP480	4	21			
	销售部	交换机	S3700	24	1	4F		
		<u>M-AP</u>	RJ-AP480	4	21			
	人事部	交换机	S3700	24	1	5F		
		<u>M-AP</u>	RJ-AP480	4	21			
	人事部、财务部、总裁办公室	交换机	S3700	24	1	6F		
		<u>M-AP</u>	RJ-AP480	4	22			
备注： <u>G-AP</u> :高密 AP <u>M-AP</u> : 面板 AP								

二、胜天公司网络总体规划

（一）方案设计原则

在网络部署过程中，我们应遵循以下几项关键原则：

（1）高性能

随着公司业务的持续扩展和计算机网络技术的不断更新，局域网所承载的业务范围日益广泛，用户数量不断增加。这要求为每个用户分配足够的带宽，以确保流畅的网络体验。面对公司多样化的业务需求，如语音、视频、邮件等，我们可以通过 QoS（服务质量）技术将不同业务分配到不同的队列中，从而最大化保障用户的流畅性。此外，通过增加链路带宽，也能更好地满足公司未来发展的需求。

（2）可扩展性

随着时间的推移和业务的扩展，公司未来有可能成长为大型上市公司。这意味着公司机房的搭建需要进行质的飞跃，因此当前的网络规划必须考虑到未来十年的发展需求。随着未来多种应用的部署，公司的系统应能够及时进行更新和迭代，以适应不断变化的业务环境。

（3）网络管理的复杂程度

通过合理规划 IP 地址、使用标准化协议以及在规划过程中综合考虑各种因素，我们应尽可能降低网络的复杂度。同时，应提前考虑未来网络中可能出现的问题，以便能够快速分析、定位并解决故障，确保网络的高效运行。

（4）安全性和可靠性

网络的安全性和可靠性是公司必须重视的关键问题，这直接关系到公司内部信息和机密信息的安全。在进行网络规划和部署时，应使用防火墙抵御黑客攻击，并通过流量策略限制不必要的部门间访问。在可靠性设计方面，通常采用冗余备份和负载分担的方式，以满足公司的需求。

（二）总体设计

1. 分层网络设计

胜天公司的网络系统从设计上分为出口防火墙、汇聚层和接入层三个部分；从

功能上可分为市场部、安保部、财务部等八大部门。

(1) 出口防火墙

防火墙作为公司的出口路由器，在中小型网络拓扑中，通常采用防火墙代替路由器作为出口设备。防火墙不仅功能丰富，还能有效抵御病毒。考虑到公司业务流量全部需要经过防火墙进行转发和检测，防火墙的性能至关重要。我们采用最新的华为防火墙，防火墙之间的链路采用万兆链路连接。

(2) 汇聚层

汇聚层作为公司各部门之间的聚集点，通常通过部署两台核心交换机进行链路聚合，以实现冗余备份。链路采用千兆链路连接。汇聚层还充当公司内部访问的转发点，不同部门之间的互访需要通过汇聚层进行转发，因此对汇聚层设备的性能要求较高。

(3) 接入层

接入层主要连接部门的终端设备，包括打印机、电脑、摄像头等。对接入层的性能要求不高，但对设备的接口数量要求极高。通常，接入层设备采用 48 端口百兆以太网接口。

2. 胜天公司网拓扑结构

根据上述分析，胜天公司的网络布线设计采用多层星型结构和点到点连接。这种设计确保了当任何一条线路或设备出现故障时，都不会影响公司业务的正常转发，也不会对其他部门的业务造成影响。我们建议采用华为的 USG9500 系列高端防火墙作为公司的出口防火墙，汇聚层采用华为的 S5700 交换机，接入层采用华为的 S3700 交换机。

胜天公司网拓扑图如图 2.1 所示：

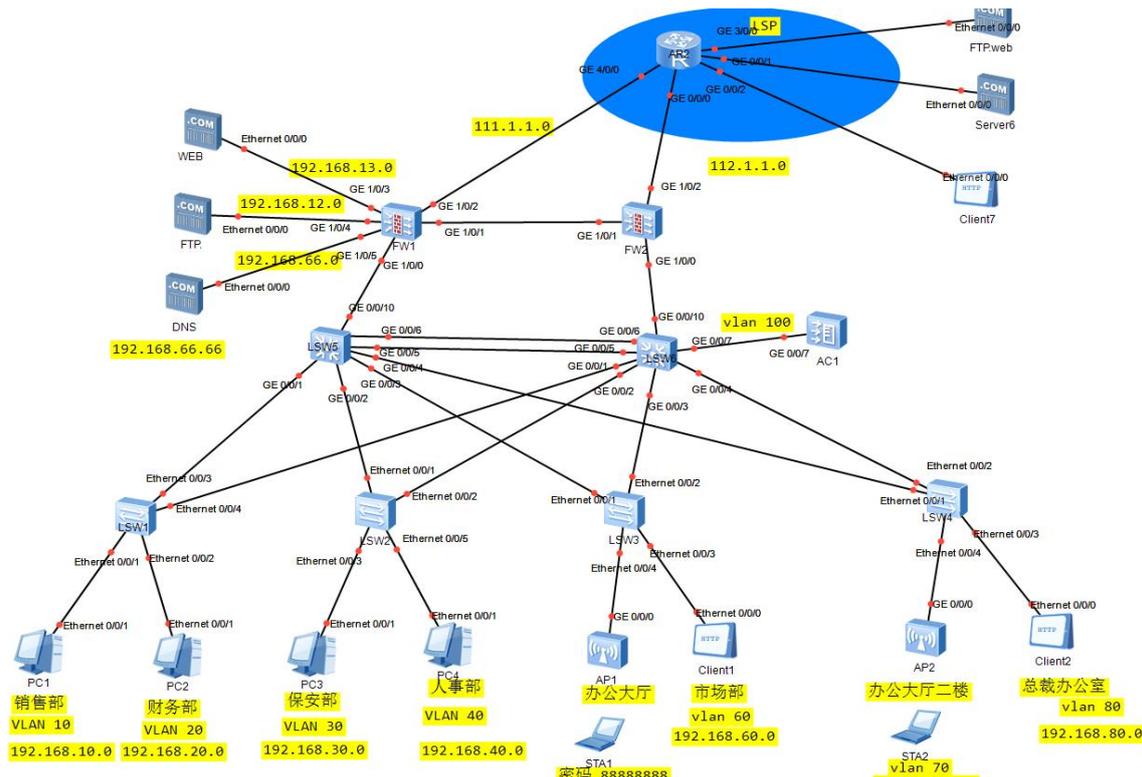


图 2.1 胜天公司网拓扑图

(三) 网络技术选型

在胜天公司网络建设中，主干网技术的选择对整个网络的运行至关重要。选择适合公司需求的主流网络技术，不仅能确保网络的高性能，还能保证其先进性和扩展性，为未来向新技术的平滑过渡提供保障，从而保护投资。目前，成熟的局域网技术包括以太网、高速以太网（快速以太网和千兆以太网）、万兆以太网、FDDI、Token Ring 和 Token Bus 等，而广域网中的 ATM 也是一种可选技术。

由于公司部门众多，若所有部门都处于同一广播域，交换机性能会显著下降。因为交换机以广播方式发送数据，当终端发送 ARP 广播包时，所有交换机都会接收到该广播包，但只有目标交换机会响应，这无疑占用了大量链路资源。为解决这一问题，我们采用 VLAN 技术，将一个交换机划分为多个逻辑广播域，使不同 VLAN 之间处于不同的广播域。这样，ARP 广播包仅在所属 VLAN 内转发，有效减少了广播流量，提高了网络效率。

在设计网络拓扑时，为增强网络的健壮性，我们通常采用冗余组网方式，但这可能会引发环路问题。此时，STP（生成树协议）技术可派上用场。当交换机组成环形拓扑时，环路可能引发广播风暴。默认情况下，交换机收到未知单播帧会进行

泛洪处理。若网络中的交换机收到重复数据帧，会导致 MAC 地址表频繁刷新，出现震荡，甚至可能使交换机瘫痪或死机。

公司规模较大，员工众多，但运维人员仅有 1-2 人。在传统以太网中，若管理员采用静态配置 IP 地址的方式使 PC 上网，面对数百台 PC，管理员需逐一配置，工作效率极低。若员工对网络参数不熟悉，私自更改 IP 地址，导致 IP 地址冲突，将增加管理员的管理负担。在企业网络中，静态配置 IP 地址会导致地址使用效率低下，部分地址长期闲置，造成浪费。

为实现公司内网的互联互通，我们可采用静态路由或动态路由。鉴于静态路由配置复杂、扩展性差，我们选择使用动态路由协议 OSPF。

随着互联网的快速发展和人口增长，人手一台笔记本电脑成为常态，但 IPv4 地址有限，已无法满足日益增长的上网需求。为解决这一问题，开发出了 NAT（网络地址转换）技术。该技术可将内网地址转换为公网地址，既能满足上网需求，又能缓解 IPv4 地址短缺的问题。

1.网络设备选型

（1）防火墙

各服务器通过 10Gbps 双绞线与防火墙相连，确保网络的安全性和高性能。

（2）部门接入交换机

财务部、市场部、保安部等每个部门均配备 2 台接入交换机，以满足部门内部的网络需求。

（3）无线接入点（AP）

办公大厅和办公大厅二楼部署多个 AP 设备，确保外来人员能够通过无线网络方便地接入互联网。

（4）接入层与汇聚层连接

接入层交换机通过千兆链路汇聚层交换机相连，确保数据传输的高效性和稳定性。

2.网络抗干扰性

根据上述分析，胜天公司的网络具有较强的抗干扰性。即使链路出现断开或故障，备用路径的存在也能确保业务流量的正常访问。我们采用华为设备进行公司网络的规划与设计，确保网络的高性能和可靠性。

通过以上技术选型和设备部署，胜天公司的网络系统不仅能够满足当前的业务需求，还具备良好的扩展性和可靠性，为公司未来的发展提供了坚实的基础。

三、胜天公司网络工程建设

网络工程建设主要涵盖网络设备选型、VLAN 规划以及网络设备总体规划等方面。以下是详细说明：

(1) 网络设备选型

胜天公司由大客户投资扩建，公司共分为人事部、市场部、财务部等八个部门。每个部门的业务流量、人数和业务需求各不相同。在经济因素的考量下，我们综合考虑了各部门的业务流量、安全性和设备作用等因素，进行了合理的设备选型，旨在最大化提升公司网络的性价比。

(2) 服务器

根据胜天公司的网络需求，我们选择了基于 Intel 系列的深信服厂商的服务器。深信服 VDS-R-7550 型服务器具备卓越的业务灵活性和强大的承载能力。它能够将 CPU、内存、存储等硬件资源虚拟化为资源池，并根据需求将资源分配给各个虚拟机终端，以承载业务流量。深信服 VDS-R-7550 型服务器的具体参数如表 3.1 所示。

深信服 VDS-R-7550 型服务器参数如表 3.1 所示：

表 3.1 VDS-R-7550 型服务器参数

产品类别	深信服 VDS-R-7550
服务器类型	机架式服务器
服务器结构	2U
CPU 类型	至强 金牌
CPU 型号	Gold 6226R
CPU 频率	2.90 GHz
CPU 核心	16 核心
硬盘热拔插盘	支持
内存类型	DDR4
最大内存容量	24*32G
标准接口	4xUSB 接口、 1xVGA 接口

(3) 核心交换机

鉴于公司的业务流量需求，我们选用华为 S5700 系列交换机作为公司的汇聚层设备。S5700 系列交换机能够实现有线无线的深度融合，支持对用户的统一管理，具备全面的 QoS 策略、高数据转发端口以及高扩展性和可靠性。

S5700 交换机主要参数如表 3.2 所示：

表 3.2 S5700 交换机参数

产品类别	S5703
交换容量	38.4/168Tbps
包转发率	7200/36000Mpps
冗余设计	主控、电源、监控板、风扇框（前后及左后风道）
无线管理	支持随板 AC 支持 AP 接入控制、AP 域管理和 AP 配置 QoS、安全和用户管理支持 AC 功能分层部署
用户管理	支持统一用户管理、PPPoE、802.1X、MAC、Portal 认证方式、基于流量和时长计费方式、分组分域分时授权方式
路由特性	支持三层网络协议、IPv4 与 IPv6 双协议栈
缓存容量	支持每端口 200ms 数据缓存
数据中心特性	支持 TRILL, FCoE (DCB), EVN, nCenter, EVB, SPB, VXLAN 等数据中心特性

（4）接入交换机

接入层交换机采用华为 S3700 交换机。接入层对设备性能要求不高，主要负责终端设备的数据转发。根据胜天公司的具体需求，选择 S3700 交换机在性价比方面更具优势。

S3700 交换机主要参数如表 3.3 所示。

表 3.3 S3700 交换机参数

产品类型	以太网交换机
交换容量(Gpbs) 64Gpbs	64Gpbs
端口数	24
模块插槽数	1
交换方式	存储转发
包转发率	9.3Mpps
端口类型	22 个 10/100Base-TX, 2 个千兆 Combo 口 (10/100/1000Base-T 或 100/1000Base-X), 上行接口卡可选 2 端口千兆光口卡

（5）防火墙

华为 USG9500 系列是华为推出的下一代防火墙产品。该系列产品不仅具备传统防火墙的所有功能，而且在硬件和芯片性能上有了显著提升，报文检测能力也得到

了增强。此外，USG9500 还引入了 PI 深度报文检测（IPS 入侵防御）、AV 反病毒、URL 过滤、邮件过滤、文件内容检查、VPN、NAT、上网行为管理以及报表和日志功能等。

USG9500 防火墙主要参数如表 3.4 所示。

表 3.4 USG9500 防火墙主要参数

防火墙类型	下一代防火墙
产品型号	USG9500
产品类型	企业级级, 硬件防火墙, VPN 防火墙, 万兆级防火墙
最大吞吐量	10000Mbps
安全过滤带宽	300Mbps
外形尺寸	455×430×88mm
重量	9.8Kg
硬件参数	PIII 900 , 256M SDRAM, 32M DOM, 4 个 10/100Base-TX LAN 口
固定接口	4 个 10/100Base-TX LAN 口
用户数限制	无用户数限制
并发连接数	800000 并发连接数
VPN	支持 VPN 功能
功能特点	包过滤, NAT, 透明应用代理, 路由, 网桥或透明连接, 端口映射, 双极热备, 流量控制, 宽管理, IP 与 MAC 地址绑定, 防止地址欺骗, 实时监控, 日志审计, 入侵监测, 灾难恢复。

通过上述设备选型，胜天公司的网络系统不仅能够满足当前的业务需求，还具备良好的扩展性和可靠性，为公司未来的发展提供了坚实的基础。

(1) 无线 AC、AP

根据公司要求，无线接入控制器（AC）和接入点（AP）的性能指标需达到高标准，以确保在办理业务时能为客服提供更优质的服务。因此，我们选择华为的 AC6005 作为无线接入控制器。该设备具备高转发能力、大吞吐量、高无线用户接入能力，并支持直接转发和隧道转发，从而更好地保障数据流量的安全性。此外，它还支持多种无线协议。对于 AP，我们选用锐捷 RJ-AP850 作为用户接入点，其能够高效转发业务流量，性价比高，并且能更好地兼容不同版本型号的 AC。

(2) VLAN 规划

VLAN（虚拟局域网）是一种能够隔离广播域的技术，可将一个网络划分为多个

独立的虚拟网络。这些独立的虚拟网络之间不能随意访问，必须遵循预定义的 VLAN 规则。如果两个 VLAN 的 PVID（默认 VLAN ID）相同，则可以相互访问；如果 PVID 不同，则需要检查接口是否允许该 VLAN 通过。如果允许，则打上相应的 PVID；否则，数据包将被丢弃。

根据公司要求，为更好地管理各部门，我们使用 VLAN 技术将各部门划分到独立的网络中，确保部门之间不能随意访问。特别是财务部和总裁办公室，这两个部门的网络访问权限受到严格限制。此外，通过划分 VLAN，我们能够有效避免广播域的出现，从而显著提高网络设备的性能，减轻设备处理大量业务流量的负担，延长设备的使用寿命。

公司的 VLAN 划分如下表 3.5 所示：

表 3.5 VLAN 规划表

LAN	VLAN 名称	IP 段	默认网关	备注	LAN
VLAN60	SCB	192.168.60.0/24	192.168.60.254	市场部	VLAN60
VLAN10	XSB	192.168.10.0/24	192.168.10.254	销售部	VLAN10
VLAN40	RSB	192.168.40.0/24	192.168.40.254	人事部	VLAN40
VLAN30	BAB	192.168.30.0/24	192.168.30.254	保安部	VLAN30
VLAN20	CWB	192.168.20.0/24	192.168.20.254	财务部	VLAN20
VLAN50	BGDD	192.168.50.0/24	192.168.50.254	办公大厅	VLAN50
VLAN80	ZCBGS	192.168.80.0/24	192.168.80.254	总裁办公室	VLAN80
VLAN70	BGDTEL	192.168.70.0/24	192.168.70.254	办公大厅二楼	VLAN70

（3）网络设备规划

一个成功的项目不仅体现在网络拓扑的规划、部署与实施上，网络设备的合理规划同样至关重要。合理的设备规划能够减少资源浪费，提高网络设备的性能，实现资源的高效利用。需要注意的是，在实际网络规划中，通常不考虑其他自治系统（AS）的规划。由于本次网络规划与设计是在模拟器中进行的，因此，外网 ISP 以外的设备不在本次规划范围内。胜天公司的网络设备规划详情如表 3.6 所示：

表 3.6 胜天公司设备规划

项目名称	设备名称	设备型号	接口数量	设备数量
胜天公司	二层交换机	S3700	24	13
	核心交换机	S5703	24	2
	防火墙	USG9500	4	2
	AC	AC-6005	24	1
	AP	RJ-AP850	1	10
		RJ-AP480	1	80
	FTP 服务器	VDS-R-7550	5	1
	WEB 服务器			1
	DNS 服务器			1

通过以上规划，胜天公司的网络系统不仅能够满足当前的业务需求，还具备良好的扩展性和可靠性，为公司未来的发展提供了坚实的基础。

四、网络实现

(一) 服务器配置

由于用户使用的终端设备和操作系统存在差异，文件传输和共享存在诸多限制。为此，我们部署了 FTP 服务器，以解决文件传输障碍问题。FTP 服务器的配置如图 4.1 所示：

Web 服务器通常指网站服务器，其主要功能是向浏览器等 Web 客户端提供文档，放置网站文件供网络用户浏览，并提供可下载的数据文件。Web 服务器能够将图形、音频、视频信息集成于一体，用户只需点击链接即可在不同站点间切换。Web 服务器的配置如图 4.2 所示：

核心交换机的主要作用是加快大型局域网内部的数据交换，其路由功能也服务于这一目的，能够实现一次路由、多次转发。核心交换机的配置命令如下：



图 4.1 FTP 配置

Web 服务器通常指网站服务器，它的主要作用是向浏览器等 Web 客户端提供文

档，放置网站文件让网络用户浏览以及提供可以下载的数据文件。Web 可以将图形、音频、视频信息集合于一体，只需要从一个链接点击另一个链接就能各站点切换。

WEB 服务器配置如图 4.2:



图 4.2 WEB 服务器配置

(二) 核心交换机配置

核心交换机的作用是加快大型局域网内部的数据交换，所具有的路由功能也是为这目的服务的，能够做到一次路由，多次转发，配置命令如下。

```
#syname sw5 //设备命名为 sw5
#vlan batch 10 15 20 30 40 50 56 60 70 80 //批量创建 vlan
#stp instance 0 root primary //将实例 0 设备设为根桥设备
#stp instance 10 root primary //将实例 10 设备设为根桥设备
#stp instance 20 root primary //将实例 20 设备设为根桥设备
#dhcp enable //开启 dhcp 服务
#stp region-configuration //进入 mstp 配置
#region-name lyl //实例名称
#revision-level 12 //实例级别
#instance 10 vlan 10 20 30 40 //vlan10 20 30 40 加入到实例 10
#instance 20 vlan 50 60 70 80 100 //vlan50 60 70 80 100 加入到实例 20
```

```

#active region-configuration //激活配置
#ip pool 10 //进入地址池给地址池一个名称
#gateway-list 192.168.10.254 //地址池分配网络范围
#network 192.168.10.0 mask 255.255.255.0 //下发 DNS 的地址
#dns-list 192.168.66.66 8.8.8.8
#interface Vlanif 10 //配置三层接口 vlanif
#ip address 192.168.10.253 255.255.255.0 //配置 IP 地址
#vrrp vrid 10 virtual-ip 192.168.10.254 //配置虚拟 IP 地址
#vrrp vrid 10 priority 150 //配置虚拟 IP 优先级
#dhcp select global //开启下发 dhcp 服务功能
#interface Vlanif15 //创建 vlanif 功能
#ip address 192.168.15.5 255.255.255.0 //配置 IP 地址
#ospf network-type p2p //将 ospf 的链路类型改成 p2p
#ospf 1 router-id 5.5.5.5 //配置 ospf 的 router id
#silent-interface Vlanif10 //配置成静默接口, 防止发送无效报
#stp region-configuration //进入 mstp 配置
#region-name lyl //实例名称
#revision-level 12 //实例级别
#instance 10 vlan 10 20 30 40 //vlan10 20 30 40 加入到实例 10
#instance 20 vlan 50 60 70 80 100 //vlan50 60 70 80 100 加入到实例 20
#active region-configuration //激活配置
#ip pool 10 //进入地址池给地址池一个名称
#gateway-list 192.168.10.254 //地址池分配网络范围
#network 192.168.10.0 mask 255.255.255.0 //下发 DNS 的地址
#dns-list 192.168.66.66 8.8.8.8
#interface Vlanif 10 //配置三层接口 vlanif
#ip address 192.168.10.253 255.255.255.0 //配置 IP 地址
#vrrp vrid 10 virtual-ip 192.168.10.254 //配置虚拟 IP 地址
#vrrp vrid 10 priority 150 //配置虚拟 IP 优先级
#dhcp select global //开启下发 dhcp 服务功能
#interface Vlanif15 //创建 vlanif 功能
#ip address 192.168.15.5 255.255.255.0 //配置 IP 地址
#ospf network-type p2p //将 ospf 的链路类型改成 p2p
#ospf 1 router-id 5.5.5.5 //配置 ospf 的 router id
#silent-interface Vlanif10 //配置成静默接口, 防止发送无效报文

```

(三) 二层交换机配置

二层交换机负责决定最优路由和转发数据帧，配置命令如下：

```

#sysname SW1 //设备命名为 sw1
#vlan batch 10 20 //创建 vlan10 20
#stp region-configuration //进入 mstp 配置
# region-name lyl //命名
#revision-level 12 //设置级别
#instance 10 vlan 10 20 30 40 //vlan10 20 30 40 加入到实例 10 中

```

```
#instance 20 vlan 50 60 70 80 100 // vlan10 20 30 40 加入到实例 20 中
#active region-configuration //激活配置
#acl number 3000 //配置 acl 规则
#rule 5 deny icmp destination 192.168.20.0 0.0.0.255
//匹配拒绝的目的地址 icmp 的流量
rule 6 deny icmp destination 192.168.80.0 0.0.0.255 rule 10 permit icmp //
未匹配的 icmp 流量全部放行
#
#interface Ethernet0/0/1
#port link-type access //将接口划分到 asccess 模式
#port default vlan 10 //将接口划分到 vlan10 中
#traffic-filter inbound acl 3000 //调用流量政策
#interface Ethernet0/0/3
#port link-type trunk //将接口类型改为 trunk 类型
#port trunk allow-pass vlan 10 20 //允许的 vlan 通过
```

(四) 出口防火墙配置

防火墙可以限制他人进入内部网络，过滤掉不安全服务和非法用户，配置如下。

FW1 配置

```
#syname FW1 //防火墙设备命名
#hrp enable //开启心跳线
#hrp interface GigabitEthernet1/0/1 remote 1.1.1.2 //心跳线对端地址
#hrp mirror session enable
#hrp standby config enable
#hrp track interface GigabitEthernet1/0/0 //检测的接口
#hrp track interface GigabitEthernet1/0/2 //检测的接口
#firewall zone local //本地安全区域
#set priority 100 //安全区域优先级
#firewall zone trust //进入 trust 区域
#set priority 85 //区域默认优先级
#add interface GigabitEthernet0/0/0 //将接口加入到安全区域
#add interface GigabitEthernet1/0/0 //将接口加入到安全区域
#ip route-static 0.0.0.0 0.0.0.0 111.1.1.2
//配置到互联网的静态缺省出口路由
#nat server 2 protocol udp global 10.10.10.10 dns
//将内部 DNS 服务器的私网地址映射到公网
#inside 192.168.66.66 dns
#nat server 1 protocol tcp global 111.1.1.100 ftp inside 192.168.12.2 ftp no-reverse
//将 ftp 服务器映射到公网中
#nat server 1 protocol tcp global 111.1.1.10 ftp inside 192.168.13.3 www //将
http 服务器的私网地址映射到公网中
#nat address-group 1 0 //配置地址池
#mode pat //模式
#section 0 111.1.1.10 111.1.1.15 //地址池的范围
```

```

#security-policy //进入安全策略
#rule name LYL //策略名称（内部用户访问互联网所需的安全策略）
#source-zone trust //配置源区域
#destination-zone untrust //配置目的区域
#source-address 192.168.0.0 mask 255.255.0.0 //允许通过的源地址
#service dns //允许通过的 DNS 服务
#service ftp //允许通过的 FTP 服务
#service http //允许通过的 http 服务
#service icmp //允许通过的 ping 包
#action permit //允许
#nat-policy //NAT 策略
#rule name LYL //策略名称
#source-zone dmz //匹配源区域
#source-zone trust //匹配源区域
#destination-zone untrust //匹配的目的区域
#source-address 192.168.0.0 mask 255.255.0.0 //匹配源地址
#service dns //允许通过的 DNS 服务
#service ftp //允许通过的 FTP 服务
#service http //允许通过的 http 服务
#service icmp //允许通过的 ping 包
#action source-nat address-group 1 //通过源 NAT 技术进行转
    
```

（五）ISP 路由器配置

ISP 路由器 AR2 配置，负责本地安全区域和安全区域优先级。

AR2 配置

[V200R003C00]

```

#sysname lsp //设备命名
#firewall zone Local //本地安全区域
Priority 15 //安全区域优先级
#ip route-static 10.10.10.10 255.255.255.255 111.1.1.1 //配置静态路由
#ip route-static 111.1.1.0 255.255.255.0 111.1.1.1 //配置静态路由
#ip route-static 10.1.1.0 255.255.255.0 112.1.1.1 //配置静态路由
    
```

五、网络测试

(一) 物理网络连通测试

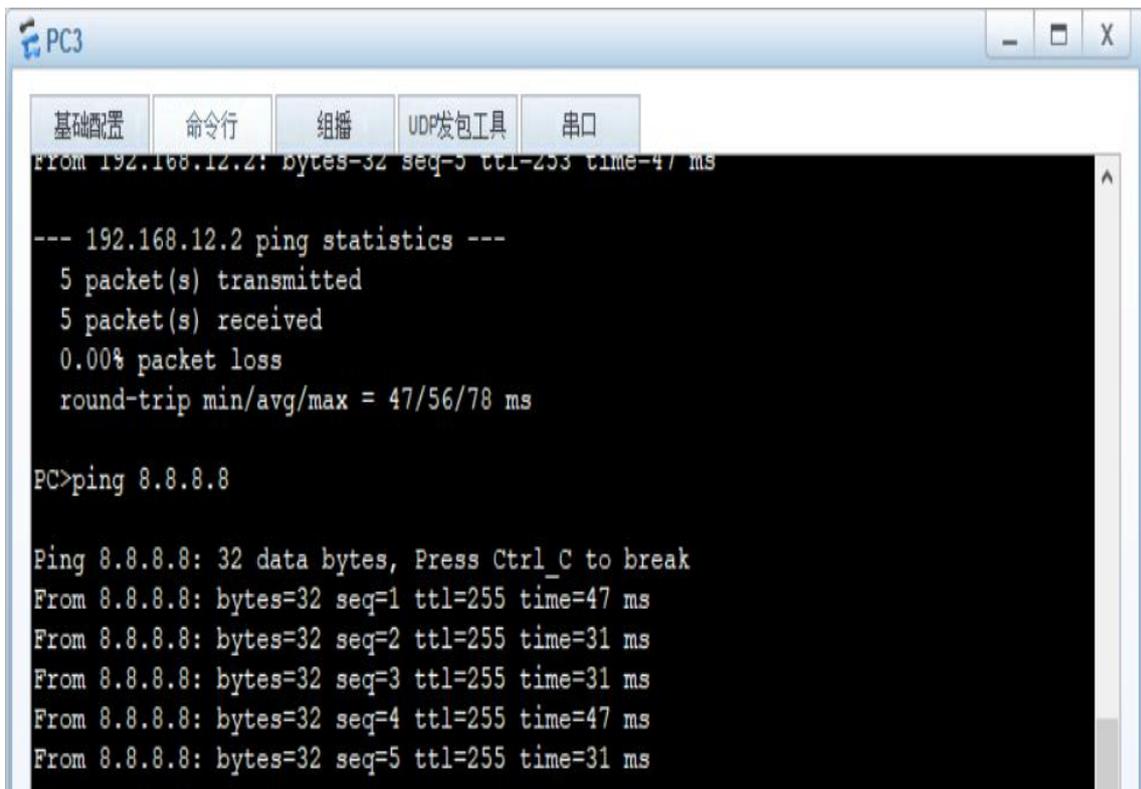
测试目的：检测网络的链路连通性

测试方式：通过 PC 或移动设备动态获取 IP 地址后，使用 Ping 命令和 ICMP 协议测试 32 字节数据包的传输反馈。

测试步骤及结果：随机选择部门 PC 或无线设备，使用 Ping 命令测试公司内核心交换机、防火墙及外部网络的连通性。测试结果显示，响应时间均在 10 毫秒以内。

测试结论：物理网络已成功联通，核心交换机能够与其他设备正常通信。

(1) 核心交换机连通性测试（管理地址为 8.8.8.8/32）如下图 5.1 所示：



```

PC3
基础配置  命令行  组播  UDP发包工具  串口
from 192.168.12.2: bytes=32 seq=5 ttl=253 time=47 ms

--- 192.168.12.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 47/56/78 ms

PC>ping 8.8.8.8

Ping 8.8.8.8: 32 data bytes, Press Ctrl_C to break
From 8.8.8.8: bytes=32 seq=1 ttl=255 time=47 ms
From 8.8.8.8: bytes=32 seq=2 ttl=255 time=31 ms
From 8.8.8.8: bytes=32 seq=3 ttl=255 time=31 ms
From 8.8.8.8: bytes=32 seq=4 ttl=255 time=47 ms
From 8.8.8.8: bytes=32 seq=5 ttl=255 time=31 ms
    
```

图 5.1 核心交换机测试

(2) 防火墙连通性测试（管理地址为 9.9.9.9/32）如下图 5.2 所示：

```

PC3
基础配置 命令行 组播 UDP发包工具 串口
--- 8.8.8.8 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/37/47 ms

PC>clear
Invalid command!

PC>ping 9.9.9.9

Ping 9.9.9.9: 32 data bytes, Press Ctrl_C to break
From 9.9.9.9: bytes=32 seq=1 ttl=254 time=63 ms
From 9.9.9.9: bytes=32 seq=2 ttl=254 time=62 ms
From 9.9.9.9: bytes=32 seq=3 ttl=254 time=63 ms
From 9.9.9.9: bytes=32 seq=4 ttl=254 time=47 ms
From 9.9.9.9: bytes=32 seq=5 ttl=254 time=62 ms

--- 9.9.9.9 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 47/59/63 ms
    
```

图 5.2 防火墙机测试

(3) ISP 运营商连通性测试（管理地址为 2.2.2.2/32）如下图 5.3 所示：

```

PC4
基础配置 命令行 组播 UDP发包工具 串口

PC>ping 2.2.2.2

Ping 2.2.2.2: 32 data bytes, Press Ctrl_C to break
From 2.2.2.2: bytes=32 seq=1 ttl=253 time=78 ms
From 2.2.2.2: bytes=32 seq=2 ttl=253 time=46 ms
From 2.2.2.2: bytes=32 seq=3 ttl=253 time=47 ms
From 2.2.2.2: bytes=32 seq=4 ttl=253 time=47 ms
From 2.2.2.2: bytes=32 seq=5 ttl=253 time=47 ms

--- 2.2.2.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 46/53/78 ms

PC>
    
```

图 5.3 ISP 运营商测试

（二）无线网络连通性测试

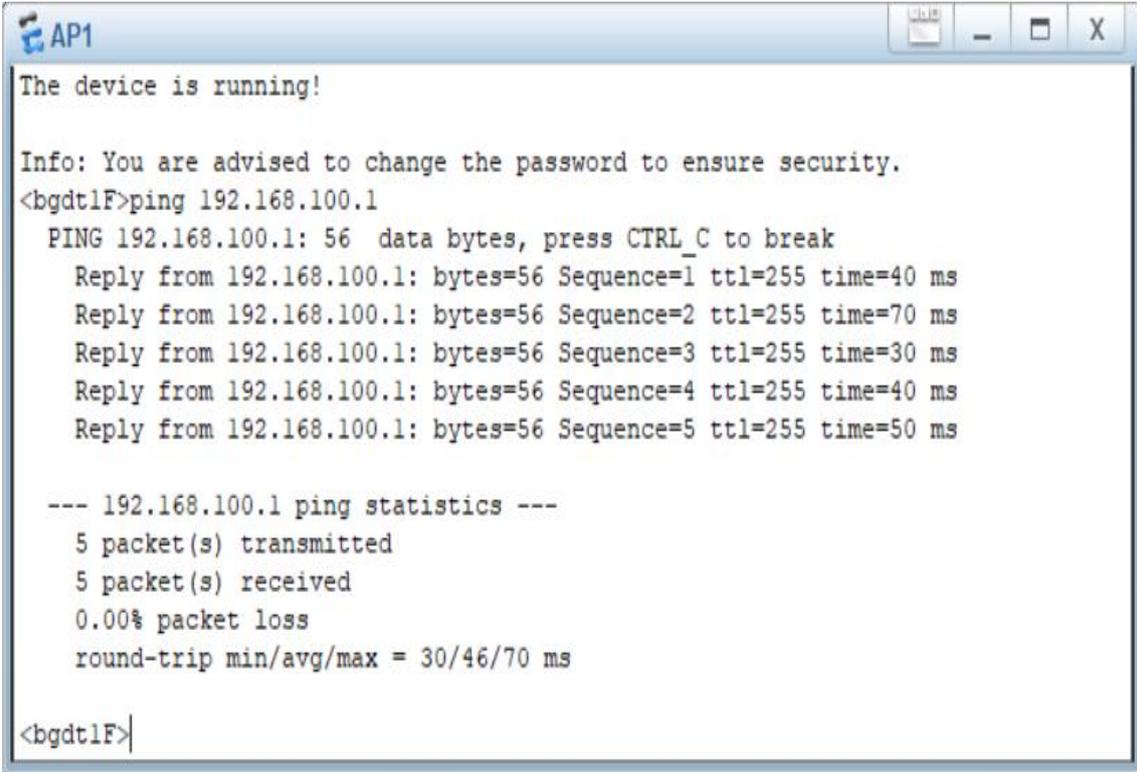
测试目的：检查 AC 设备是否与内网互通，以及 AC 是否成功下发配置给 AP 设备。

测试方式：使用终端 PC 或电话动态获取 IP 地址后，对 AC 设备和 AP 设备进行 Ping 测试，检查是否有反馈信息。

测试步骤及结果：随机选择部门 PC 或无线设备，使用 Ping 命令测试公司内部终端节点到无线 AC 设备、AP 设备到无线 AC 设备的连通性。测试结果显示，响应时间均在 10 毫秒以内。

测试结论：各部门无线网络已实现互通，各 PC 之间可以正常通信。

（1）AC 连通性测试（管理地址为 192.168.100.1/24）如下图 5-4 所示。



```

AP1
The device is running!

Info: You are advised to change the password to ensure security.
<bgt1F>ping 192.168.100.1
  PING 192.168.100.1: 56 data bytes, press CTRL_C to break
    Reply from 192.168.100.1: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 192.168.100.1: bytes=56 Sequence=2 ttl=255 time=70 ms
    Reply from 192.168.100.1: bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 192.168.100.1: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 192.168.100.1: bytes=56 Sequence=5 ttl=255 time=50 ms

--- 192.168.100.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 30/46/70 ms

<bgt1F>
    
```

图 5.4 AC 测试

（三）AP 上线测试

测试目的：通过 AC 下发配置指令，使 AP 发射无线射频，确保 STA 无线终端能够正常接入并访问外部网络（ISP 运营商地址 2.2.2.2/32）。

测试方式：如图 5-5 所示，通过 AC 下发配置指令，使 AP 发射无线射频，STA

无线终端能够正常接入并访问外部网络。

测试结论：AP 设备成功上线，无线终端能够正常接入并访问外部网络。

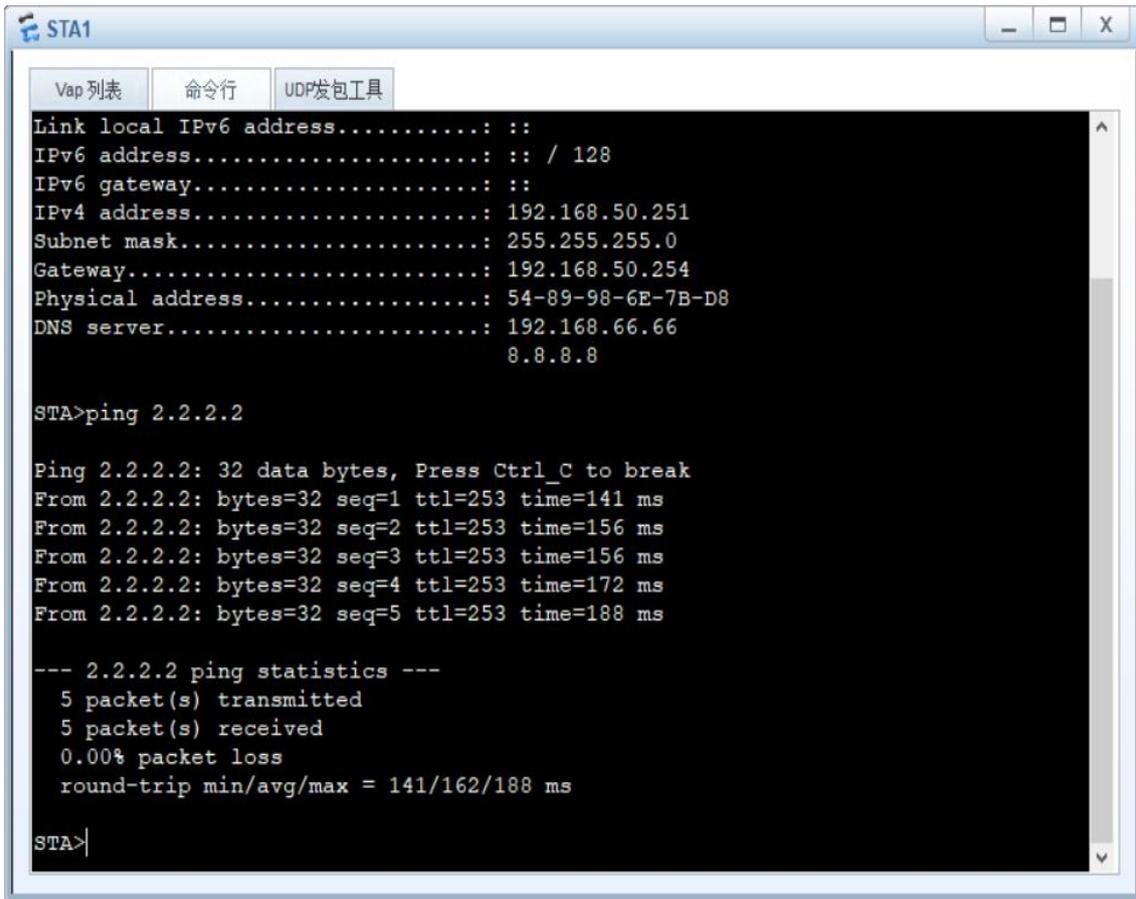


图 5.5 AP 上线测试

(四) 服务器网测试

测试目的：测试公司总部、分部以及外部用户是否能够正常访问公司总部的服务器设备。

测试方式：在总部和分部使用客户端通过 DNS 将内部服务器的地址和域名进行映射，使内部客户端可以通过域名访问内部 Http 服务。同时，通过 FTP 服务器的 IP 地址直接访问 FTP 业务。

测试步骤及结果：在分部客户端页面输入内部域名地址，如果能够正常访问且服务器响应迅速，则表示访问无问题。内部客户端直接通过 FTP 服务器的 IP 地址访问 FTP 服务，如果能够快速响应并访问，则表示 FTP 服务正常。外部客户端通过公网地址和域名地址进行映射，输入 IP 地址后能够正常进行文件的下载和上传，且速度较快，证明 FTP 服务正常。

测试结论：经测试，FTP 服务器和 WEB 服务器均能正常运行，公司总部、分部及外部用户均能顺利访问公司服务器。

测试结论：经以上测试 FTP 服务器和 WEB 服务器可以正常运行。

(1) WEB 服务器测试如下图 5-6 所示。

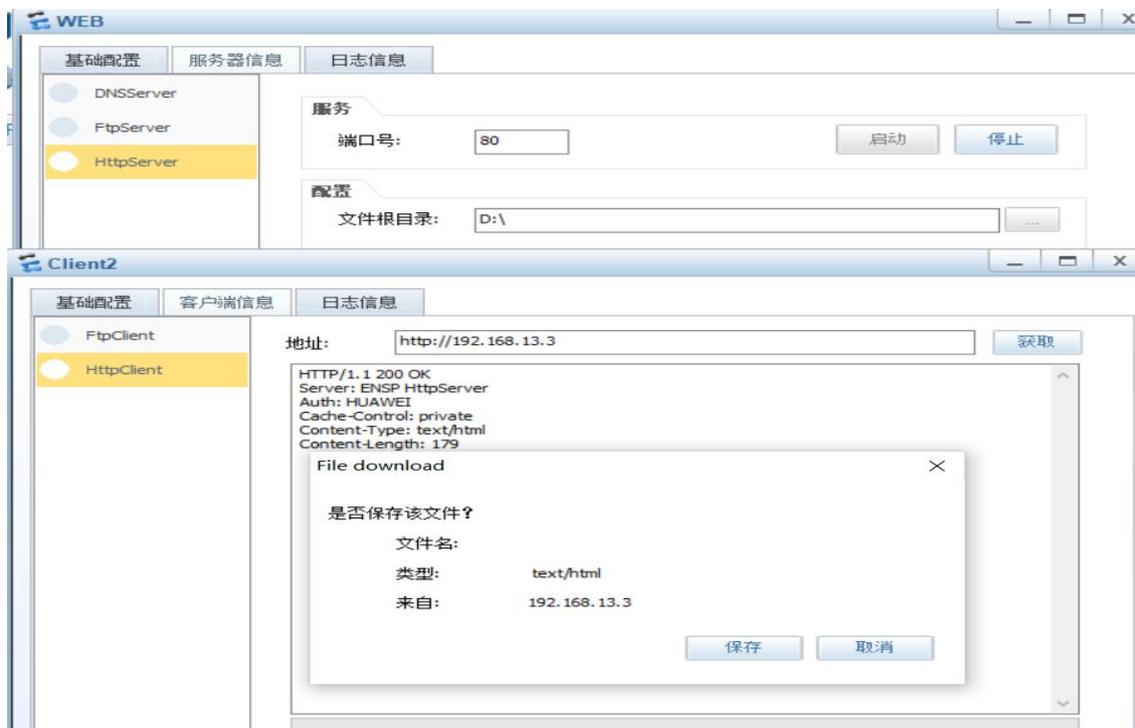


图 5.6 WEB 服务器测试

(2) FTP 服务器测试如下图 5.7 所示。

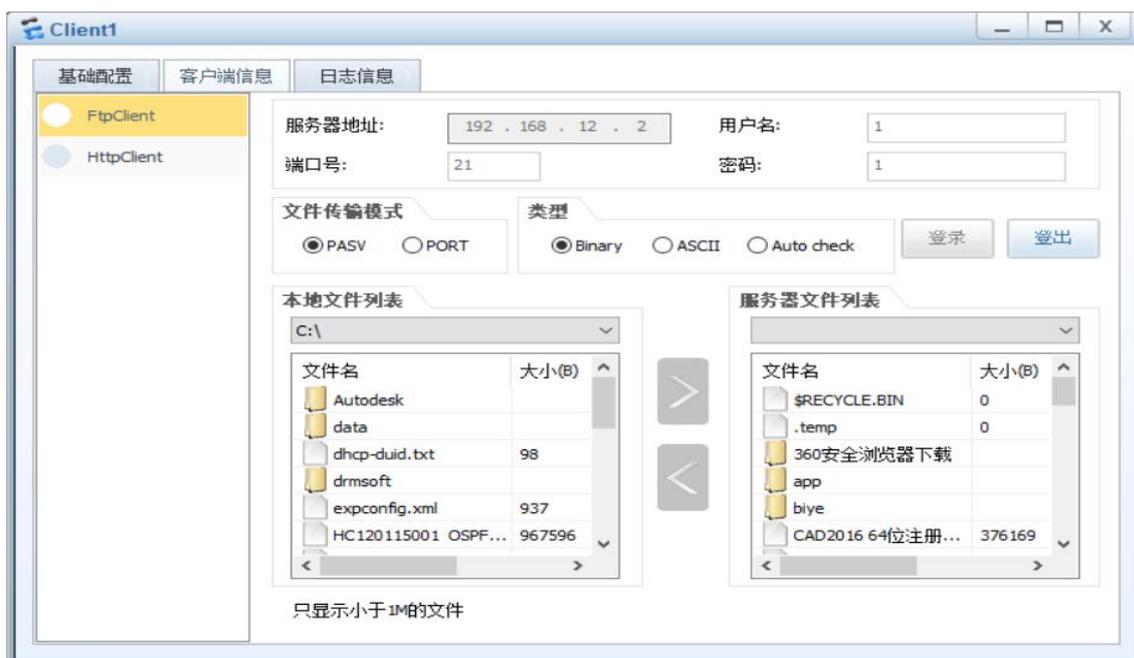
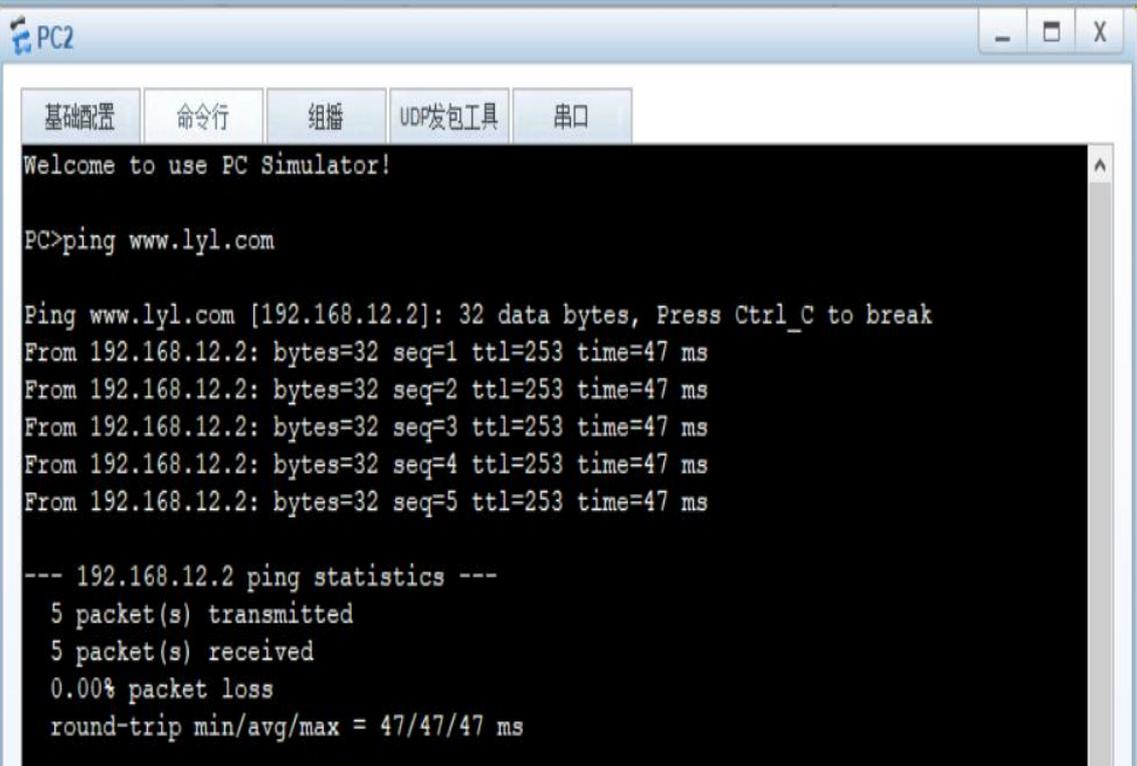


图 5.7 FTP 服务器测试

(3) DNS 服务器测试如下图 5.8 所示。



```
PC2
基础配置  命令行  组播  UDP发包工具  串口
Welcome to use PC Simulator!
PC>ping www.lyl.com
Ping www.lyl.com [192.168.12.2]: 32 data bytes, Press Ctrl_C to break
From 192.168.12.2: bytes=32 seq=1 ttl=253 time=47 ms
From 192.168.12.2: bytes=32 seq=2 ttl=253 time=47 ms
From 192.168.12.2: bytes=32 seq=3 ttl=253 time=47 ms
From 192.168.12.2: bytes=32 seq=4 ttl=253 time=47 ms
From 192.168.12.2: bytes=32 seq=5 ttl=253 time=47 ms
--- 192.168.12.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 47/47/47 ms
```

图 5.8 DNS 服务器测试

通过以上配置和测试，胜天公司的网络系统不仅能够满足当前的业务需求，还具备良好的扩展性和可靠性，为公司未来的发展提供了坚实的基础。

六、总结

通过本次毕业设计，我对网络工程规划设计的基本流程有了较为深入的理解，收获颇丰。以下是我在设计过程中的一些体会：

（1）全局观念的重要性

网络工程规划设计需要具备强烈的全局观念。这不仅意味着要明确网络的层次结构，如接入层、汇聚层和核心层，还需深入思考各层之间的管理策略，以确保网络的扩展性和健壮性。接入层作为连接各部门信息节点的关键部分，应选择性价比高、接口丰富的设备，以满足基本需求。核心层则承担着公司业务的中枢角色，所有网络业务均需通过核心层进行转发。因此，核心层设备必须具备高速转发能力、高接口速率、大吞吐量，并能在突发事件中保持稳定，不丢包。

（2）设备选型的针对性

设备选型应紧密结合公司的实际情况，进行有针对性的选择。接入层设备主要负责连接各部门的信息节点，因此应选择性能适中、接口数量充足且价格合理的设备，以满足基本的网络连接需求。核心层设备则是公司业务的中枢，所有网络业务都需经过核心层进行转发。因此，核心层设备应具备高速转发能力、高接口速率、大吞吐量，并能在突发事件中保持稳定，不丢包。此外，核心层设备还应具备冗余备份和负载均衡功能，以确保网络的高可用性。

（3）域名访问的安全性

使用域名访问是提升公司网络安全性的重要手段。通过域名解析，可以有效控制各部门和外部网络的信息节点对公司 FTP 和 Web 业务的访问，避免未经授权的访问和潜在的安全风险。域名访问不仅提高了网络的安全性，还增强了网络的可管理性，使得网络管理员能够更高效地监控和管理网络流量。

（4）VLAN 技术的应用

VLAN 技术在隔离广播域和提高网络性能方面发挥了重要作用。通过将公司各部门划分到不同的 VLAN 中，可以有效减少广播流量，避免链路带宽的浪费，同时提高网络访问的安全性。VLAN 的划分不仅有助于网络的管理和维护，还能根据业务需求灵活调整网络配置。

（5）冗余设计的重要性

在网络设计中，冗余设计是确保网络高可用性的关键。通过在关键节点部署冗

余设备，如防火墙、核心交换机等，可以有效避免单点故障，确保网络在设备故障时仍能正常运行。冗余设计不仅提高了网络的可靠性，还减少了因设备故障导致的业务中断时间。

（6）测试与优化

在完成网络设计和设备部署后，进行全面的测试和优化是确保网络稳定运行的重要环节。通过测试，可以发现并解决潜在的问题，优化网络性能。测试内容包括物理网络连通性测试、无线网络连通性测试、AP 上线测试以及服务器访问测试等。这些测试不仅验证了网络的连通性和设备的性能，还为后续的优化提供了依据。

通过本次毕业设计，我不仅掌握了网络工程规划设计的基本流程，还深刻理解了全局观念、设备选型、域名访问、VLAN 技术、冗余设计以及测试与优化的重要性。这些知识和经验将为我未来的职业发展打下坚实的基础。

参考资料

- [1] 曹吉龙. 计算机网络的可靠性优化[J]. 电子世界, 2023 (09) :45-47.
- [2] 苏海娜. 网络系统安全维护策略研究[J]. 北华航天工业学院学报, 2023 (06) :33-35.
- [3] 高伟东, 彭涛. TD-SCDMA 无线网络规划优化及无线资源管理[M]. 人民邮电出版社, 2024. 09.
- [4] 黄允凯, 谈英姿. 深入浅出 NetLinx 网络架构[M]. 机械工业出版社, 2023. 08.
- [5] 李琦. 宜家酒店网络设计方案[J]. 湖南开放大学, 2024. 11.
- [6] 胡启龙. 嘉禾职业中专网络规划方案[J]. 湖南开放大学, 2024. 08.
- [7] 张威龙. 龙门中学校园网实施方案[J]. 湖南开放大学, 2024. 12.
- [8] 王惠郡. 不器有限责任公司网络规划与设计[J]. 湖南开放大学, 2023. 06.
- [9] 唐勇. 天启网络科技企业网络设计方案[J]. 湖南开放大学, 2024. 01.
- [10] 邹志荣. 富满科技公司网络构建设计方案[J]. 湖南开放大学, 2023. 04.