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：湘创公司内部局域网设计方案

学生姓名 罗烨林

学生学号 010425171779

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）：罗烨林　日　期：2025.5.13

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）：[illegible]　日　期：2025.5.15

（注：本页学生和指导教师须亲笔签名。）

目　录

一、 项目概述

（一）公司背景

湘创公司是一家专注于健康产品营销的企业。随着当代人对个人健康的关注度不断提高，公司的业务迎来了快速增长，员工数量也迅速增加。这种快速的发展使得原有的网络系统难以满足日益增长的业务需求。为了应对这一挑战，公司高层要求信息管理部对现有网络进行全面重新规划，以提升网络性能并实现统一管理。

湘创公司的组织结构经过重新调整，现有七个部门分布在三层办公区域。具体分布如下：总经办、法务部和财务部位于第一层；人资行政部和信息管理部位于第二层；市场部和客服部位于第三层。此外，公司还计划建立一个分部，并与合作公司卫数开展业务往来，实现信息化数据的互联互通。

（二）公司网络现状问题

湘创公司目前拥有四台思科路由器、一台三层交换机和两台二层交换机。随着公司规模的扩大和业务的拓展，原有的网络结构和设备配置已无法满足当前的需求。具体问题如下：

（1）网络结构与组织分布不匹配：现有的网络架构未能充分适应公司新的组织结构和业务需求，导致网络管理复杂且效率低下。

（2）设备老化与性能瓶颈：部分网络设备已使用多年，性能逐渐下降，难以支持公司业务的快速增长，尤其是在高峰时段，网络拥堵现象频发。

（3）缺乏冗余设计：当前网络缺乏必要的冗余机制，一旦关键设备或链路出现故障，将直接影响公司的正常运营，增加业务中断的风险。

（4）安全与管理挑战：随着公司业务的数字化转型，网络安全和数据保护的重要性日益凸显。现有的网络系统在安全策略和管理功能上存在不足，难以有效应对日益复杂的网络威胁。

（三）设计目标与最终实现

为了满足公司未来三至五年的战略发展需求和业务模式，我们对现有网络进行了全面的升级改造。具体目标和实现措施如下：

（1）优化部门划分与网络管理

重新梳理部门划分，明确各管理区域的网络需求，合理分配网络资源，确保每个部门都能获得高效、稳定的网络服务。通过精细化的网络管理，提升整体运营效率。

（2）实现网络互通与技术管理

采用先进的网络技术和设备，实现公司内部各部门之间的高效网络互通。同时，通过技术手段对网络通信进行精细化管理，确保关键业务的优先级和数据传输的稳定性。此外，建立与合作公司卫数的专用网络连接，实现信息化数据的无缝对接，提升业务协同效率。

（3）提升网络可靠性和性能

引入冗余设计，包括设备冗余和链路冗余，确保网络在关键设备或链路出现故障时仍能正常运行，最大限度减少业务中断时间。同时，升级网络设备，提升网络带宽和处理能力，满足公司业务快速增长的需求，为员工提供高速、稳定的网络体验。

通过以上措施，湘创公司的网络系统将得到全面优化，不仅能够满足当前的业务需求，还能为公司的长期发展提供坚实的技术支持。

二、 需求分析

（一）需求概述

据分析调研湘创公司概况与日后发展参见表 2.1 和表 2.2，需作以下改进。

表 2.1 公司总部组织结构前后概况

组织结构 分布	湘创公司原概况	湘创公司需改善概况
一层	总经办、财务部	总经办、法务部、财务部
二层	人资行政部 （含信息管理组）、 市场客服部	人资行政部、信息管理部
三层		市场部、客服部

表 2.2 公司新构建网络互通概况

组织 网络概况	湘创公司	分部公司	合作公司卫数公司
内网数据互通	分部公司	湘创公司	
仅能访问 DMZ 网络区域	卫数公司	卫数公司	湘创公司

鉴于现有设备的实际情况，我们决定在延用原有设备的基础上，对湘创公司的整体网络架构进行重新设计。具体方案如下：

新增核心交换机：新增一台高性能核心交换机，作为网络的核心节点，负责汇聚和转发全公司各楼层的网络流量。

替换汇聚交换机：更换原有的五台汇聚交换机，以满足各楼层的网络需求。这些汇聚交换机将分布在各楼层，负责连接核心交换机和接入层交换机。

接入层交换机：继续使用原有的 13 台接入层二层交换机，为各楼层的终端设备提供网络接入服务。这些交换机将连接到相应的汇聚交换机。

分部公司备用交换机：公司原有的二层交换机将放置在分部公司，作为备用接入交换机使用，以应对突发情况，确保网络的高可用性。

（二）可行性分析

1、 公司组织环境需求分析

湘创公司原组织结构由 5 个部门组成，分布在 2 层办公区。具体分布如下：

第一层：总经办、财务部。

第二层：人资行政部（含 IT 组）、市场部。

随着公司组织结构的调整，现共建有 7 个部门，分布在 3 层办公区：

第一层：总经办、法务部、财务部。

第二层：人资行政部、信息管理部。

第三层：市场部。

此外，公司规模的扩大还要求建立一个分部公司，并与合作公司卫数开展业务往来，实现数据互通。这种组织结构和业务需求的变化，对网络架构提出了更高的要求。

2、 网络规模需求分析

每个部门分处不同的楼层与工作区域，所需的信息点数量也各不相同。为了满足未来 3-5 年的网络需求，我们设计了一个详细的网络需求框架。各部门所需的信息点数量如表 2.3 所示：

表 2.3 湘创公司组织结构及信息点概况

部门	信息点数量
总经办	20
法务部	15
财务部	18
人资行政部	22
信息管理部	25
市场部	30
分部公司	10
总经办	20

3、 网络功能需求分析

企业网络不仅是一个局域网，也是一个广域网。它将分散的部门或工作组网络与公司内部网络互连，使公司内的所有计算机用户能够访问任何数据或计算资源。根据湘创公司的发展规划，网络需要实现以下功能：

内部网络互通

实现公司各楼层和各部门之间的高效网络互通，确保数据传输的稳定性和可靠性。

分部公司数据互通

确保公司总部与分部公司之间的数据互通，支持远程办公和业务协同。

与合作公司卫数的数据互通

与合作公司卫数进行业务往来，实现数据的无缝对接。为确保信息安全，湘创公司与分部公司只能与合作公司卫数相互访问 DMZ 网络区域。

网络安全与管理

引入先进的网络安全策略，确保网络的高可用性和数据的安全性。通过技术手段对网络通信进行精细化管理，确保关键业务的优先级和数据传输的稳定性。

通过以上设计和分析，湘创公司的网络架构将能够满足当前和未来的业务需求，为公司的持续发展提供坚实的技术支持。

（三）网络设备的选型

设备选型及数量如表 2.4。

表 2.4 设备选型及数量

序号	产品类型	产品型号		总数量
1	核心交换机	RG-S7805C	1、主控引擎与业务板卡完全物理分离,采用全分布式转发处理架构,独立主控引擎插槽≥2 个，独立业务插槽数≥3 个；此次配置千兆光≥24 个，配置万兆光口≥36,配置主控引擎≥2，配置电源模块≥2；此次配置板载千兆交换网络 48 口。 2、交换容量≥30Tbps，包转发性能≥6500Mpps。以官网最低为准。 3、 支持多对一镜像,基于流的镜像，一对多镜像。支持 SPAN、RSPAN 远程镜像，支持 VLAN 的镜像。 4、支持 IPv6 静态路由、RIPng、OSPF v3、BGP4+等路由协议。 5、 完善的虚拟化功能：N:1 虚拟化：可将 2 台物理设备虚拟化为 1 台逻辑设备,虚拟组内设备具备统一的二层及三层转发表项，统一的管理界面,并可实现跨设备链路聚合，1：N 虚拟化：可将一台物理设备虚拟化为多台逻辑设备,各虚拟交换机间具备独立的转发表项及配置界面,各虚拟交换机的配置/重启互不影响。	1

序号	产品类型	产品型号		总数量
			6、 支持专门针对 CPU 的保护机制，能够针对发往 CPU 处理的各种报文进行流量控制和优先级处理，保护交换机在各种环境下稳定工作。 7、支持专门基础网络保护机制（非 CUP 保护），增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的 CPU 负载，从而保障整个网络的稳定运行。 8、单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥52，提高槽位利用率和业务可靠性。 9、要求整机 ARP 表项≥20K，实供板卡必须满足此项要求。 10、 为保障核心设备的安全可靠性，所投交换机需支持 6KV 以上防雷击能力。	
2	汇聚交换机	RG-S5760-24SFP4XS-L	1、交换容量≥672Gbps。 2、包转发率≥156Mpps。 3、固化 100/1000M SFP 光接口≥24 个，10G/1G SFP+光接口≥4 个。 4、为保证设备在受到外界机械碰撞时能够正常运行，要求所投交换机 IK 防护测试级别至少达到 IK05。 5、要求所投产品端口浪涌抗扰度≥10KV（即具备 10KV 的防雷能力）。 6、支持静态路由、RIP/RIPng、OSPFv2/OSPFv3 等三层	5

序号	产品类型	产品型号		总数量
			路由协议。 7、支持 SNMP、CLI(Telnet/Console)、RMON、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web。 8、支持专门基础网络保护机制,能够限制用户向网络中发送数据包的速率,对有攻击行为的用户进行隔离,保证设备和整网的安全稳定运行。 9、配置双电源。	
3	接入交换机 24 口 千兆交换机	RG-S2910-24GT4SFP-L	弱三层接入交换机，24 个 10/100/1000M 自适应电口，4 个 1G SFP 光口，固化交流电源和风扇。	13
4	机柜		≥36U，机柜深≥800mm.	2

三、 方案设计与规划

（一）网络拓扑设计

根据需求分析设计网络拓扑概览如图 3.1。

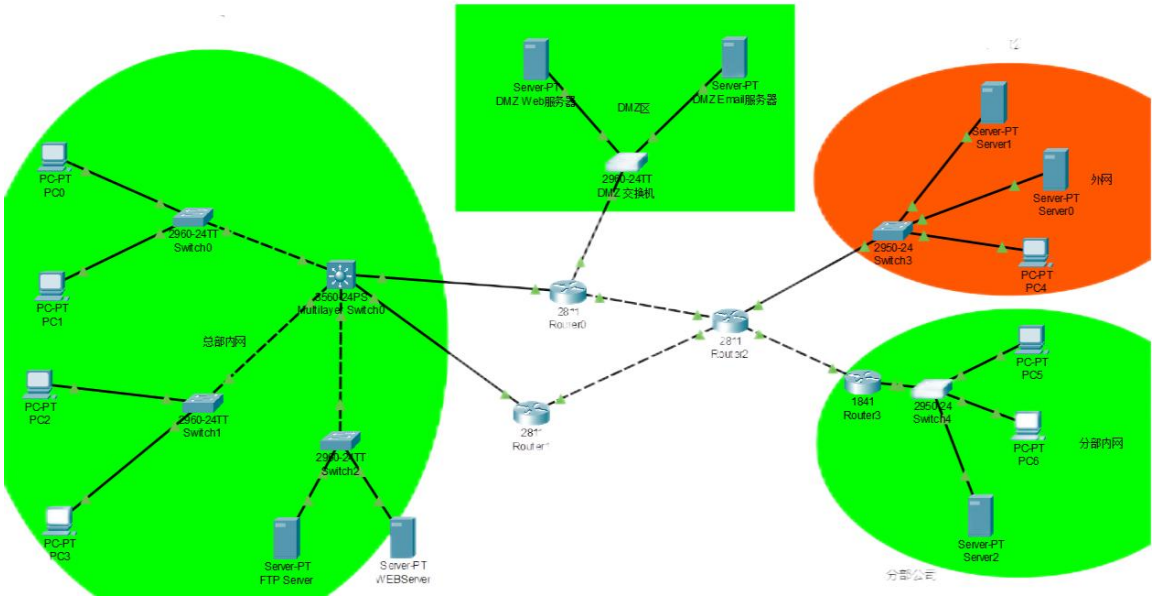

图 3.1 网络拓扑设计概览

（二）网络 IP 地址与 VLAN 规划

因公司管理不考虑信息化的深入投入须要易于维护管理，公司更注重业务的发展及管理的灵活性。故各部门 VLAN 不做子网划分，仅作网段管理。如表 3.1 所示：

表 3.1 网段规划

分布	湘创公司需改善概况	网段规划
总部一层	总经办	192.168.11.0/24
	法务部	192.168.12.0/24
	财务部	192.168.13.0/24
总部二层	人资行政部	192.168.14.0/24

分布	湘创公司需改善概况	网段规划
	信息管理部 （含 机房）	192.168.15.0/24
总部 三层	市场部	192.168.16.0/24
	客服部	192.168.17.0/24
	分部公司	192.168.21.0/24
	合作公司卫数	192.168.31.0/24

（三）企业组网（安全）策略

为了构建一个高效、安全且可扩展的企业网络，我们制定了以下详细的安全策略：

（1）网络区域划分与按需互通

根据表 2.2 的设计，我们将网络划分为三个主要区域：企业内网、DMZ 区和互联网。每个区域根据业务需求实现按需互通，确保网络资源的高效利用和数据传输的安全性。通过合理的网络规划，实现各区域之间的高效通信，同时避免不必要的数据流动，降低安全风险。

（2）内网隔离与保护

采用基于 VLAN 的内网隔离策略，将不同部门和业务的网络流量进行逻辑划分。通过 VLAN 技术，确保各部门之间的网络流量相互隔离，防止内部网络攻击和数据泄露。同时，为每个 VLAN 配置独立的访问控制策略，进一步增强内网的安全性。

（3）内网路由互通

利用 OSPF（开放最短路径优先）协议实现内网路由的高效互通。OSPF 协议能够动态计算网络中的最短路径，确保数据包能够快速、准确地到达目的地。通过配置 OSPF，实现内网各区域之间的无缝路由，提高网络的稳定性和可靠性。

（4）内网结构隐藏

通过 NAT（网络地址转换）技术隐藏内网结构，确保内网的真实 IP 地址对外部网络不可见。NAT 技术不仅可以节省公网 IP 地址资源，还能有效防止外部攻击者获取内网的详细信息，从而提高网络的安全性。

（5）企业异地内网互联

采用 VPN（虚拟专用网络）技术实现企业异地内网之间的安全互联。通过 VPN，企业总部与分部公司之间可以建立加密的通信隧道，实现数据在公网上的安全传输。即使数据在公网中传输，也能确保其保密性和完整性，如同在私有网络中一样安全。

（）区域访问策略

制定企业内网、互联网及 DMZ 区之间的区域访问策略，明确各区域之间的访问权限和数据流向。通过访问控制列表（ACL）和防火墙规则，限制不必要的访问请求，确保网络的安全性。例如，内网用户可以访问互联网，但互联网用户不能直接访问内网资源；DMZ 区的服务可以被互联网访问，但内网用户对 DMZ 区的访问受到严格限制。

（6）DMZ 区服务对外网可见

将 DMZ 区的服务配置为对外网可见，同时确保这些服务的安全性。DMZ 区通常用于部署对外提供服务的服务器，如 Web 服务器、邮件服务器等。通过合理的安全配置，确保这些服务在对外提供服务的同时，不会暴露内网的敏感信息，防止外部攻击者利用 DMZ 区的漏洞入侵内网。

通过以上策略，湘创公司的企业网络将具备高效、安全和可扩展的特点，能够满足公司当前及未来的发展需求。

四、 网络技术与实现

（一）链路模式设置

核心交换机：

SWA(config)#int ran f0/1-20,21,31 # 进入接口范围配置模式，选择 FastEthernet 0/1 到 0/20、0/21 和 0/31 这些接口进行批量配置

SWA(config-if)#switchport trunk encapsulation dot1q # 配置所选接口的 Trunk 封装类型为 802.1Q（dot1q）

SWA(config-if)#switchport mode trunk # 将所选接口的模式设置为 Trunk 模式

SWA(config-if)#exit # 退出接口配置模式，返回到全局配置模式

SWA(config)#

汇聚交换机（具有代表性设备配置，f0/23 为上行链路接口，f0/24 为下行链路接口）：

sw (config)#int f0/23 # 进入 FastEthernet 0/23 接口的配置模式

sw (config-if)# switchport mode trunk # 将接口 0/23 的模式设置为 Trunk 模式

sw (config)#int f0/24 # 进入 FastEthernet 0/24 接口的配置模式

sw (config-if)# switchport mode trunk # 将接口 0/24 的模式设置为 Trunk 模式

sw (config-if)#exit

sw (config)#

（其他汇聚交换机配置相同，此处不重复）

（二）VLAN 技术

SWA#vlan database # 进入 VLAN 数据库配置模式

SWA(vlan)#vlan 11 na Vlan11 # 创建 VLAN 11，并将其名称设置为 "Vlan11"

VLAN 11 modified:

Name: Vlan11 # 系统确认 VLAN 11 已被修改，名称为 "Vlan11"

SWA(vlan)#vlan 12 na Vlan12 # 创建 VLAN 12，并将其名称设置为 "Vlan12"

VLAN 12 added:

Name: Vlan12 # 系统确认 VLAN 12 已被添加，名称为 "Vlan12"

SWA(vlan)#vlan 13 na Vlan13 # 创建 VLAN 13，并将其名称设置为 "Vlan13"

VLAN 13 added:

Name: Vlan13 # 系统确认 VLAN 13 已被添加，名称为 "Vlan13"

SWA(vlan)#vlan 14 na Vlan14 # 创建 VLAN 14，并将其名称设置为 "Vlan14"

VLAN 14 added:

Name: Vlan14 # 系统确认 VLAN 14 已被添加，名称为 "Vlan14"

SWA(vlan)#vlan 15 na Vlan15 #同上

VLAN 15 added:

Name: Vlan15

SWA(vlan)#vlan 16 na Vlan16 #同上

VLAN 16 added:

Name: Vlan16

SWA(vlan)#vlan 17 na Vlan17 #同上

VLAN 17 added:

Name: Vlan17

SWA(vlan)#vlan 21 na Vlan21 #同上

VLAN 21 added:

Name: Vlan21

SWA(vlan)#vlan 31 na Vlan31 #同上

VLAN 31 added:

Name: Vlan31

SWA(vlan)#exit

APPLY completed.

Exiting....

（三）VTP 技术

核心交换机：

SWA (config)#vtp version 2 # 设置 VTP（VLAN Trunking Protocol）版本为 2

SWA (config)#vtp domain tangdaixin # 将 VTP 域名设置为 "tangdaixin"

SWA (config)#vtp password tangdaixin # 设置 VTP 密码为 "tangdaixin"

SWA (config)#vtp mode server # 将交换机 SWA 的 VTP 模式设置为服务器模式

汇聚交换机（具有代表性设备配置）：

sw (config)#vtp version 2 # 设置另一台交换机 sw 的 VTP 版本为 2

sw (config)#vtp domain tangdaixin # 将交换机 sw 的 VTP 域名设置为 "tangdaixin"

sw (config)#vtp password tangdaixin # 设置交换机 sw 的 VTP 密码为 "tangdaixin"

sw (config)#vtp mode client # 将交换机 sw 的 VTP 模式设置为客户端模式

（其他汇聚交换机配置相同，此处不重复）

（四）汇聚交换机绑定接口

根据“表 3.1 网段规划”的要求，汇聚交换机（具有代表性设备配置，f0/1-20 设计为用户使用接口）为楼层交换机，“表 2.3 湘创公司组织结构及信息点概况”设计了每个楼层暂设计使用接口数。其配置如下：

汇聚交换机：

sw1 (config)#int f0/1 # 进入交换机 sw1 的 FastEthernet 0/1 接口配置模式

sw1 (config-if)# switchport mode access # 将接口 f0/1 的模式设置为 Access 模式

sw1 (config-if)# switchport access vlan11 # 将接口 f0/1 分配给 VLAN 11

sw1 (config)#int f0/2 # 进入交换机 sw1 的 FastEthernet 0/2 接口配置模式

sw1 (config-if)# switchport mode access # 将接口 f0/2 的模式设置为 Access 模式

sw1 (config-if)# switchport access vlan12 # 将接口 f0/2 分配给 VLAN 12

sw1 (config)#int f0/3 #同上

sw1 (config-if)# switchport mode access #同上

sw1 (config-if)# switchport access vlan13 #同上

sw1 (config-if)#exit

sw1 (config)#

sw2 (config)#int f0/1 #同上

sw2 (config-if)# switchport mode access #同上

sw2 (config-if)# switchport access vlan14 #同上

sw2 (config)#int f0/2 #同上

sw2 (config-if)# switchport mode access #同上

sw2 (config-if)# switchport access vlan15 #同上

sw2 (config-if)#exit

sw2 (config)#

sw3 (config)#int f0/1 #同上

sw3 (config-if)# switchport mode access #同上

sw3 (config-if)# switchport access vlan16 #同上

sw3 (config)#int f0/2

sw3 (config-if)# switchport mode access #同上

sw3 (config-if)# switchport access vlan17 #同上

sw3 (config-if)#exit

sw3 (config)#

sw4 (config)#int f0/1 #同上

sw4 (config-if)# switchport mode access #同上

sw4 (config-if)# switchport access vlan21 #同上

sw4 (config-if)#exit

sw4 (config)#

sw5 (config)#int f0/1 #同上

sw5 (config-if)# switchport mode access #同上

sw5 (config-if)# switchport access vlan31 #同上

sw5 (config-if)#exit

sw5 (config)#

接入交换机设计 f0/23 为上行链路接口，f0/24 为下行链路接口。

sw (config)#int f0/23 # 进入交换机 sw 的 FastEthernet 0/23 接口配置模式

sw (config-if)# switchport mode trunk # 将接口 f0/23 的模式设置为 Trunk 模式

sw (config)#int f0/24 # 进入交换机 sw 的 FastEthernet 0/24 接口配置模式

sw (config-if)# switchport mode trunk # 将接口 f0/24 的模式设置为 Trunk 模式

sw (config-if)#exit

sw (config)#

（五）设置 SVI 地址

SWA(config)#int vlan11 # 进入交换机 SWA 的 VLAN 11 接口配置模式

SWA(config-if)#ip add 192.168.11.254 255.255.255.0 # 为 VLAN 11 接口配置 IP 地址 192.168.11.254，子网掩码为 255.255.255.0

SWA(config)#int vlan12 # 进入交换机 SWA 的 VLAN 12 接口配置模式

SWA(config-if)#ip add 192.168.12.254 255.255.255.0 # 为 VLAN 12 接口配置 IP 地址 192.168.12.254，子网掩码为 255.255.255.0

```
SWA(config)#int vlan13
SWA(config-if)#ip add 192.168.13.254 255.255.255.0
SWA(config)#int vlan14
SWA(config-if)#ip add 192.168.14.254 255.255.255.0
SWA(config)#int vlan15
SWA(config-if)#ip add 192.168.15.254 255.255.255.0
SWA(config)#int vlan16
SWA(config-if)#ip add 192.168.16.254 255.255.255.0
SWA(config)#int vlan17
SWA(config-if)#ip add 192.168.17.254 255.255.255.0
SWA(config)#int vlan21
SWA(config-if)#ip add 192.168.21.254 255.255.255.0
SWA(config)#int vlan31
SWA(config-if)#ip add 192.168.31.254 255.255.255.0
SWA(config-if)#exit
SWA(config)#
```

（六）DHCP 技术

SWA(config)#ip dhcp pool v11 # 创建一个名为 "v11" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.11.254 # 设置 DHCP 地址池 "v11" 的默认网关为 192.168.11.254

SWA (dhcp-config)#net 192.168.11.0 255.255.255.0 # 定义 DHCP 地址池 "v11" 的网络范围为 192.168.11.0/24

SWA (dhcp-config)#ip dhcp pool v12 # 创建一个名为 "v12" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.12.254 # 设置 DHCP 地址池 "v12" 的默认网关为 192.168.11.254

SWA (dhcp-config)#net 192.168.12.0 255.255.255.0

SWA (dhcp-config)#ip dhcp pool v13 # 创建一个名为 "v13" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.13.254 # 设置 DHCP 地址池 "v13" 的默认网关为 192.168.11.254

SWA (dhcp-config)#net 192.168.13.0 255.255.255.0

SWA (dhcp-config)#ip dhcp pool v14 # 创建一个名为 "v14" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.14.254 # 设置 DHCP 地址池 "v14" 的默认网关为 192.168.11.254

SWA (dhcp-config)#net 192.168.14.0 255.255.255.0

SWA (dhcp-config)#ip dhcp pool v15 # 创建一个名为 "v15" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.15.254

SWA (dhcp-config)#net 192.168.15.0 255.255.255.0

SWA (dhcp-config)#ip dhcp pool v16 # 创建一个名为 "v16" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.16.254 # 设置 DHCP 地址池 "v16" 的默认网关为 192.168.11.254

SWA (dhcp-config)#net 192.168.16.0 255.255.255.0

SWA (dhcp-config)#ip dhcp pool v17 # 创建一个名为 "v17" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.17.254 # 设置 DHCP 地址池 "v17" 的默认网关为 192.168.11.254

SWA (dhcp-config)#net 192.168.17.0 255.255.255.0

SWA (dhcp-config)#ip dhcp pool v21 # 创建一个名为 "v21" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.21.254 # 设置 DHCP 地址池 "v21" 的默认网关为 192.168.11.254

SWA (dhcp-config)#net 192.168.21.0 255.255.255.0

SWA (dhcp-config)#ip dhcp pool v31 # 创建一个名为 "v31" 的 DHCP 地址池

SWA (dhcp-config)#de 192.168.31.254 # 设置 DHCP 地址池 "v31" 的默认网关为 192.168.11.254

SWA (dhcp-config)#net 192.168.31.0 255.255.255.0

SWA (dhcp-config)#exit

SWA(config)#

（七）核心交换机路由功能

核心交换机路由功能开启，配置如下：

SWA(config)#ip routing #开启路由功能

（八）NAT 技术

根据拓扑，边界路由器（Router0）上利用 NAT 来实现内网隐藏，使用端口多路复用技术（PAT）。配置如下：

//Router0

#int fa 0/0 # 进入 FastEthernet 0/0 接口的配置模式

#ip nat inside # 将 FastEthernet 0/0 接口配置为 NAT 的内部接口

#int fa 1/0 # 进入 FastEthernet 1/0 接口的配置模式

#ip nat outside # 将 FastEthernet 1/0 接口配置为 NAT 的外部接口

#exit # 退出当前接口配置模式，返回到全局配置模式

#access-list 10 permit 192.168.0.0 0.0.255.255 # 创建一个标准访问控制列表（ACL）编号为 10，允许来自 192.168.0.0/16 网段的流量

#ip nat pool PAT 200.1.1.3 200.1.1.3 netmask 255.255.255.0 # 创建一个 NAT 地址池，命名为 PAT，地址范围为 200.1.1.3 到 200.1.1.3

#ip nat inside source list 10 pool PAT overload（无 overload 表示多对多，有 overload 表示多对一）

（九）ACL 技术

内部访问控制（限制 PC2 去访问 PC0，即限制 VLAN31 去访问 VLAN17）

//在内网三层交换机上配置访问控制列表

#ip access-list extended acl_vlan11_vlan31

#10 deny icmp 192.168.31.0 0.0.0.255 192.168.11.0 0.0.0.255 echo

#20 permit any any

//将访问控制部署到端口上

#int fa0/2

#ip access-group acl_vlan10_vlan30 out

（十）OSPF 动态路由协议

在双方配置动态路由协议 OSPF（展示 R1，同理 R3）

Router#conf t # 进入全局配置模式，准备进行设备的配置

Router(config)#router ospf 1 # 启动 OSPF（开放最短路径优先）协议进程，进程号为 1

Router(config-router)#network 192.168.0.0 0.0.0.0 # 声明 OSPF 网络，将 192.168.0.0 网络加入 OSPF 路由协议

Router(config-router)#network 10.1.10.1 0.0.0.0 # 声明 OSPF 网络，将 10.1.10.1 网络加入 OSPF 路由协议

Router(config-router)#exit

Router(config)#

（十一）DMZ 区网络规划

利用静态 NAT 路由实现 DMZ 区隐藏。

//在边界路由器 Router0 上配置

#int fa0/1 # 进入 FastEthernet 0/1 接口的配置模式

#ip nat outside # 将 FastEthernet 0/1 接口配置为 NAT 的外部接口

#int fa1/0 # 进入 FastEthernet 1/0 接口的配置模式

#ip nat inside # 将 FastEthernet 1/0 接口配置为 NAT 的内部接口

#exit

#ip nat inside source static 10.10.1.1 202.10.1.2 # 配置静态 NAT 地址转换规则

#end

在边界路由器上，通过配置访问控制列表（ACL），实现内网、外网和 DMZ 区的访问控制策略，以确保网络的安全性和稳定性。具体策略如下：

（1）内网访问外网

内网的 PC 和服务器可以访问互联网，包括外网中的 Web 和 Email 服务器。这确保了内网用户能够正常进行外部网络通信。

（2）内网访问 DMZ

内网的 PC 和服务器可以访问 DMZ 区的 Web 和 Email 服务器，并对其进行管理。这允许内网用户访问 DMZ 区的服务，同时确保 DMZ 区的设备可以被内网管理员进行维护和管理。

（3）外网访问内网

外网中的任何主机都不允许访问内网的 PC 和服务器。内网是企业需要重点保护的核心区域，因此必须严格限制外网对内网的访问，以防止潜在的安全威胁。

（4）外网访问 DMZ

外网用户可以通过 DMZ 区的服务器（如 Web 和 Email 服务器）获取服务。DMZ 区作为缓冲区，允许外部用户访问特定的服务，同时保护内网不受直接访问。

（5）DMZ 访问内网

DMZ 区的主机（如 Web 服务器）不允许主动发起对内网主机（包括 PC 和服务器）的访问。这一策略防止 DMZ 区的设备被攻陷后，成为攻击内网的跳板，从而保护内网的安全。

（6）DMZ 访问外网

DMZ 区的主机不允许主动发起对外网的连接。这增加了 DMZ 区服务器被外网攻击者攻陷的难度，防止恶意代码向外网攻击者发送信息。

ACL 应用配置

将 out_acl_1 应用在 Router0 的 Fa0/0 端口上：

Fa0/0 端口通常连接到外网，out_acl_1 用于控制从外网进入内网或 DMZ 区的流量。

将 dmz_acl_1 应用在 Router0 的 Fa0/1 端口上：

Fa0/1 端口通常连接到 DMZ 区，dmz_acl_1 用于控制 DMZ 区与内网和外网之间的流量。

通过上述策略和配置，边界路由器能够有效地管理不同区域之间的访问权限，确保网络的安全性和稳定性。

ACL 配置结果如图 4.1：

```
Router>en
Router#show access-list
Standard IP access list 10
    10 permit 192.168.0.0 0.0.255.255
Extended IP access list dmz_acl_1
    10 permit tcp 10.10.1.0 0.0.0.255 any established
    20 permit tcp any 10.10.1.0 0.0.0.255
Extended IP access list out_acl_1
    10 permit tcp any 192.168.0.0 0.0.255.255 established
    20 permit tcp any 10.10.1.0 0.0.0.255
```

图 4.1 ACL 配置

（十二）VPN 技术

总部与分部之间通信（利用 VPN 来实现两分部通信），在 R1 上配置 Static p2p GRE over IPSec（同理在 R3 上配置）。如图 4.2：

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash sha
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 900
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 1234 address 0.0.0.0 0.0.0.0
Router(config)#crypto ipsec transform-set ccie esp-3des esp-
sha-hmac
Router(config)#int f0/1
Router(config-if)#crypto map tunnel
```

图 4.2 IPSec VPN

五、 网络系统测试

根据“表 2.2 公司新构建网络互通概况”的要求，测试概况如下：

（一）企业总部湘创公司内网互通测试

```
SWA#ping 192.168.11.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/38/160 ms

SWA#ping 192.168.12.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/11 ms

SWA#ping 192.168.13.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/16 ms

SWA#ping 192.168.14.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.14.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/8 ms

SWA#ping 192.168.15.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.15.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/15 ms

SWA#ping 192.168.16.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.16.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/15 ms

SWA#ping 192.168.17.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.17.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/18 ms

SWA#ping 192.168.21.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/15 ms

SWA#ping 192.168.31.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/16 ms

SWA#
```

图 5.1 企业总部湘创公司内网各网段互通测试

（二）企业总部湘创公司与分部公司网络互通测试

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::201:42FF:FEDD:775B
   IP Address.....: 192.168.11.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.11.254

PC>ping 192.168.21.254

Pinging 192.168.21.254 with 32 bytes of data:

Reply from 192.168.21.254: bytes=32 time=5ms TTL=255
Reply from 192.168.21.254: bytes=32 time=0ms TTL=255
Reply from 192.168.21.254: bytes=32 time=0ms TTL=255
Reply from 192.168.21.254: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.21.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

PC>
PC>
```

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::206:2AFF:FEC7:809B
   IP Address.....: 192.168.21.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.21.254

PC>ping 192.168.11.254

Pinging 192.168.11.254 with 32 bytes of data:

Reply from 192.168.11.254: bytes=32 time=2ms TTL=255
Reply from 192.168.11.254: bytes=32 time=0ms TTL=255
Reply from 192.168.11.254: bytes=32 time=3ms TTL=255
Reply from 192.168.11.254: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.11.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

PC>
PC>
```

图 5.2 企业总部湘创公司与分部公司网络互通测试

（三）企业总部湘创公司与卫数公司网络互通测试

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::201:42FF:FEDD:775B
   IP Address.....: 192.168.11.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.11.254

PC>ping 192.168.31.254

Pinging 192.168.31.254 with 32 bytes of data:

Reply from 192.168.31.254: bytes=32 time=0ms TTL=255
Reply from 192.168.31.254: bytes=32 time=0ms TTL=255
Reply from 192.168.31.254: bytes=32 time=0ms TTL=255
Reply from 192.168.31.254: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.31.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
PC>
```

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::260:70FF:FE9C:3282
   IP Address.....: 192.168.31.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.31.254

PC>
PC>ping 192.168.11.254

Pinging 192.168.11.254 with 32 bytes of data:

Reply from 192.168.11.254: bytes=32 time=0ms TTL=255
Reply from 192.168.11.254: bytes=32 time=0ms TTL=255
Reply from 192.168.11.254: bytes=32 time=0ms TTL=255
Reply from 192.168.11.254: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.11.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 5.3 企业总部湘创公司与卫数公司网络互通测试

（国）分部公司与卫数公司网络互通测试

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::206:2AFF:FEC7:809B
   IP Address.....: 192.168.21.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.21.254

PC>ping 192.168.31.254

Pinging 192.168.31.254 with 32 bytes of data:

Reply from 192.168.31.254: bytes=32 time=0ms TTL=255
Reply from 192.168.31.254: bytes=32 time=1ms TTL=255
Reply from 192.168.31.254: bytes=32 time=0ms TTL=255
Reply from 192.168.31.254: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.31.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
PC>
```

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::260:70FF:FE9C:3282
   IP Address.....: 192.168.31.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.31.254

PC>ping 192.168.21.254

Pinging 192.168.21.254 with 32 bytes of data:

Reply from 192.168.21.254: bytes=32 time=0ms TTL=255
Reply from 192.168.21.254: bytes=32 time=0ms TTL=255
Reply from 192.168.21.254: bytes=32 time=1ms TTL=255
Reply from 192.168.21.254: bytes=32 time=5ms TTL=255

Ping statistics for 192.168.21.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

PC>
PC>
```

图 5.4 分部公司与卫数公司网络互通测试

六、 参考资料

[1] 现代企业的网络规划和部署分析. 于江涛. 中国新通信，2023.23(22).

[2] 路由和交换技术在企业网构建中的应用. 邓劲松. 信息与电脑(理论版)，2024.11.

[3] 中小型企业网络方案设计与仿真实现. 孙娟. 科技视界，2022(24).

[4] 基于 ACL 和防火墙的网络安全访问控制的设计与实现. 邢慧芬，车辉. 曲靖师范学院学报，2024,41(3).

[5] 基于 GNS3 的 GRE over IPSec VPN 实验仿真. 杨礼. 中央民族大学学报(自然科学版)，2022.09.

[6] 网络安全技术在连锁企业中的应用. 黄海军. 网络安全技术与应用，2022(1).

[7] 基于等级保护 2.0 的中小型企业网络安全建设研究[J]. 陈勋，张德栋，赵英明，等. 铁路计算机应用，2023.10.