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：万联科技有限公司网络改造方案

学生姓名 颜琪涛

学生学号 010425171758

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）：颜琪涛　　日　期：2025.5.12

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、项目概况.....1

（一）设计背景.....1

（二）设计意义.....1

（三）设计思路.....1

二、万联科技有限公司网络升级改造需求分析.....3

（一）万联科技有限公司网络现状及存在问题.....3

（二）需求分析.....4

（三）设备选型.....5

三、网络升级改造方案设计.....8

（一）网络架构设计.....8

（二）核心层设计.....9

（三）汇聚层设计.....10

（四）划分多区域 VLAN.....11

（五）虚拟化设计.....12

（六）安全策略设计.....13

四、网络升级实施.....15

（一）核心层实施.....15

（二）汇聚层实施.....19

（三）接入层实施.....21

（四）安全策略实施.....22

五、新网络测试.....25

（一）测试目的.....25

（二）测试内容.....25

（三）测试过程.....25

（四）测试结果.....32

总结.....33

参考资料.....35

一、项目概况

（一）设计背景

万联科技有限公司是一家中外合资的现代化高新技术制药企业，成立于 2008 年，投资总额达 6520 万美元。公司专注于缓控释制剂技术的研发与生产，主要产品涵盖精神类、心脑血管系统和代谢类专科药物。厂区总占地面积为 50300 平方米，厂房和设备均符合 2010 年版《药品生产质量管理规范》。公司拥有数条口服固体药品生产线，其中一条生产线的年生产能力接近亿片。随着公司规模的快速扩张，现有的网络架构逐渐暴露出诸多问题和不足，难以满足日常生产经营的需求。因此，构建一个高性能、高稳定、可扩展的企业网络已成为公司发展的当务之急。

（二）设计意义

随着网络技术的飞速发展，以太网技术已成为局域网领域的主流技术。在其发展历程中，以太网技术经历了多个阶段，逐步奠定了其在局域网中的核心地位。在西方发达国家，千兆网络和万兆网络早已成为企业网络的标配。尽管中国的网络技术发展起步较晚，但通过多方面的人才培养和技术研究，中国的网络技术已取得了飞速进步。目前，国内大多数大型企业、运营商和高校已广泛采用千兆甚至万兆网络，但仍有一些企业仍停留在百兆网络或更低水平。随着技术的不断推进，千兆和万兆网络将逐渐成为国内企业网络的主流趋势。

近年来，思科公司凭借其强大的自主研发能力，推出了多种高新技术网络设备，成为国内网络设备市场的重要参与者。其发展不仅推动了中国网络技术的进步，也对促进中国自主研发技术的发展具有重要意义。

（三）设计思路

本设计分为六个部分，具体内容如下：

（1）研究背景与现状

第一部分介绍本设计的研究背景，包括国内外网络技术的发展现状，以及本设计的主要内容和目标。

（2）公司网络现状分析

第二部分详细分析万联科技有限公司当前的网络运行状况，指出网络架构中存在的问题，并结合公司实际情况提出网络升级的具体要求。同时，根据公司需求选择合适的网络设备。

（3）升级改造方案设计

第三部分介绍升级改造方案的设计思路。结合公司的升级改造需求，明确方案设计的目标，包括网络架构设计、设备选型、虚拟化设计以及 VLAN 规划等内容。

（4）方案实施

第四部分详细介绍方案的实施过程，以配置命令为核心，展示具体的网络设备配置方法。

（5）测试与验证

第五部分介绍升级改造完成后需进行的一系列测试工作，包括网络连通性测试、冗余性测试等，以确保升级改造后的网络能够满足预期目标。

（6）总结与展望

第六部分对整个升级改造方案进行总结，回顾项目实施过程中的关键点，并对未来网络技术的发展趋势进行展望。

二、万联科技有限公司网络升级改造需求分析

（一）万联科技有限公司网络现状及存在问题

（1）网络架构问题

万联科技有限公司目前采用的是两层网络结构，即核心层和接入层。公司网络出口使用的是思科 USG-6306 防火墙设备，而核心交换机则采用了优倍快公司的 US-48-500W 产品。办公楼、实验楼、车间和宿舍等区域的接入交换机，主要使用优倍快公司的 US-48-500W 和 US-24-250W 等型号。这些接入交换机大多通过百兆甚至更老旧的线缆连接到核心交换机。

公司主干网始建于 2008 年，网络设备陈旧，早已超出质保期。随着设备老化，维护成本不断增加，性能逐渐下降，故障率显著上升，甚至出现过网络瘫痪的情况，严重影响了公司网络的正常运行，导致业务生产频繁中断，给公司业绩带来了巨大损失。

（2）网络端口问题

随着公司生产业务的持续扩展、规模的不断扩大以及部门人员和终端电脑数量的增加，现有网络设备的端口数量已无法满足需求。部分部门甚至私自使用杂牌交换机，这不仅影响了网络的统一管理和管控，还带来了潜在的安全风险。

（3）VLAN 设计问题

由于公司网络建设时间较早，且当时的网络设计较为简陋，所有终端设备都处于同一个 VLAN 中，部门之间的网络可以互相访问。这种设计不仅暴露出严重的网络安全问题，还导致了 IP 地址资源紧张。随着信息网络技术的飞速发展，基于网络的通信和业务应用不断增加，国内对网络的需求日益增长。公司现有的单层网络结构和陈旧设备已无法满足现代网络时代的发展需求，这促使公司下定决心进行网络升级改造。

本公司网络升级前后拓扑图对比，如下图：

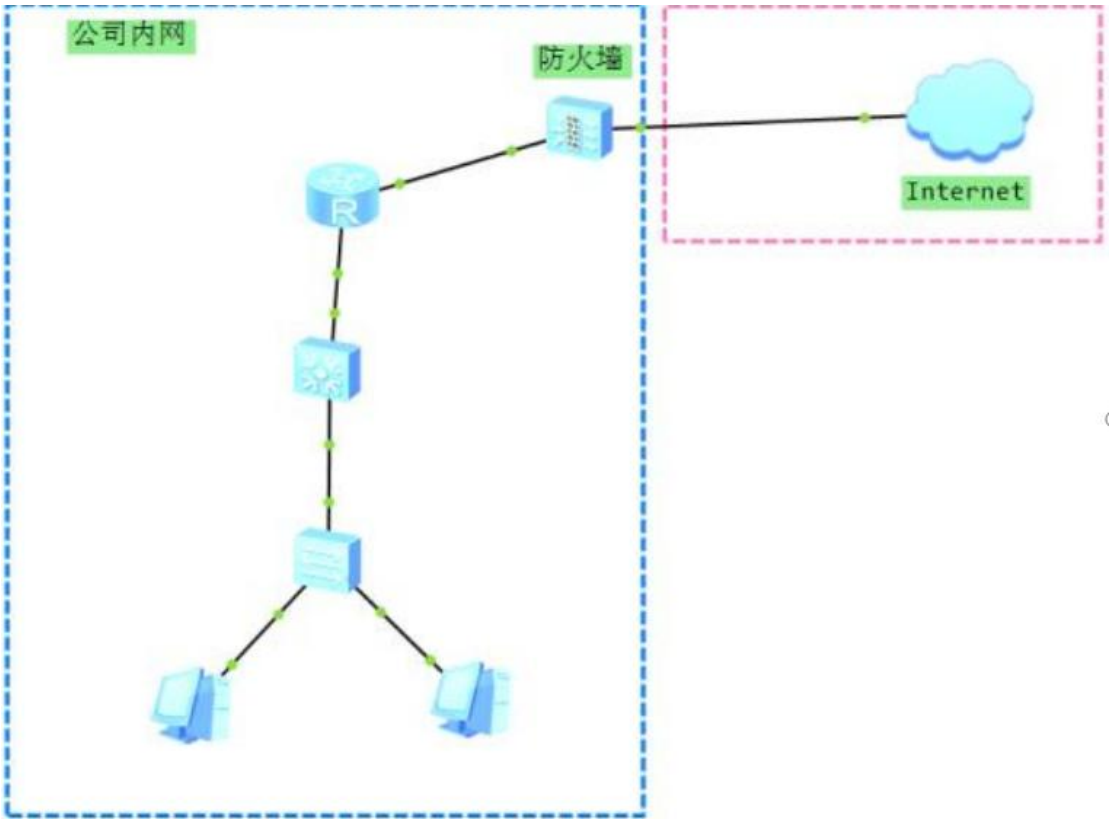

图 2.1 公司网络升级前的拓扑图

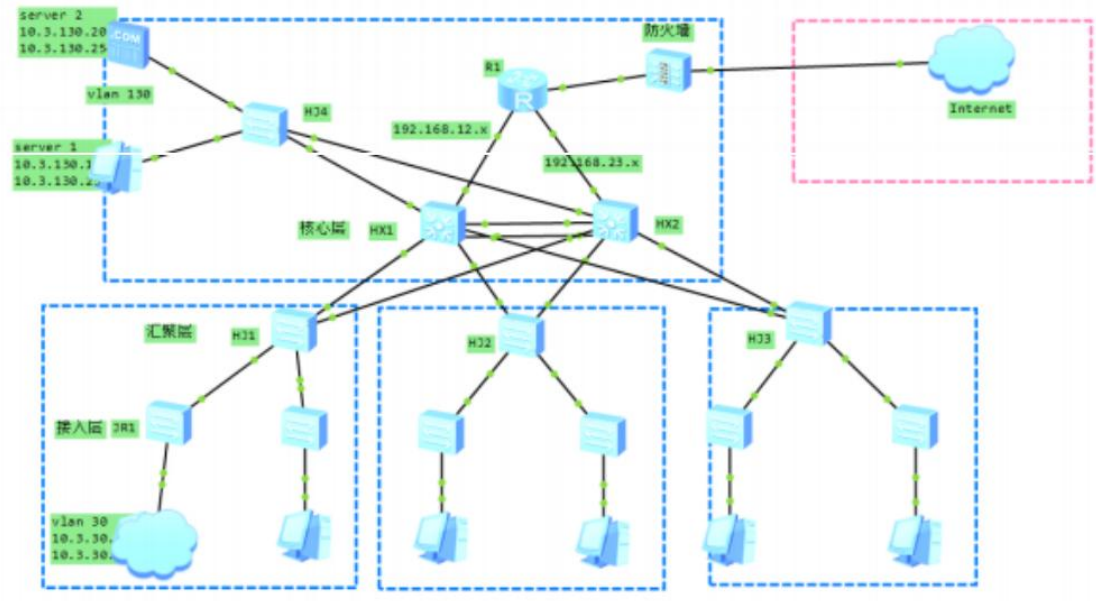

图 2.2 公司网络升级后拓扑图

（二）需求分析

随着公司业务的持续扩展，原有的网络架构存在诸多问题，如单层结构、设备

陈旧、处理性能低下以及单节点故障可能导致网络瘫痪等隐患。结合公司当前及未来的业务需求，提出以下网络升级改造需求：

（1）主干网络设备升级

更换公司主干网络设备，以提升主干网的整体性能，增加带宽和端口数量，确保公司网络的高性能、高可靠性和高稳定性。

（2）采用分层组网

公司网络采用接入层、汇聚层和核心层的三层组网方式，以提高网络的层次化管理能力和扩展性。

（3）双归链路设计

采用双汇聚加双核心的双归链路设计，提升网络可靠性，实现链路级和设备级的负载均衡与冗余备份，同时合理利用网络带宽。

（4）VLAN 划分

对公司各部门和各区域网络进行 VLAN 划分，以提高数据安全性，防范网络风暴，解决 IP 地址不足问题，并优化网络管理。

（5）访问控制策略

对公司的重要设备和系统部署访问控制策略，确保网络安全。

（三）设备选型

（1）核心交换机

公司网络区域涵盖办公、实验、生产、监控和宿舍等五大板块。核心层设备主要负责主干网络之间的高速流量传输，通常具备高速、可靠和冗余的特性。为确保公司网络的稳定性和扩展性，选择两台思科 S7908 型交换机作为核心层设备。该设备提供高端的处理性能，支持万兆端口类型，最大交换容量可达 86.4Tbps，包转发率最高为 26400Mpps，支持最多 6 个业务板卡插槽，为未来网络扩展提供了坚实基础。此外，该设备支持 IPv4/IPv6 双协议部署，确保公司业务不受网络协议限制。

图 2.3 思科 S7908 设备外观图

2、汇聚交换机

汇聚层设备位于核心层与接入层之间，上连核心层设备，下连接入层设备。其主要功能是汇聚接入层的流量数据，并根据需求转发至核心层设备。因此，汇聚层设备需要具备高性能和高转发速度。此次升级方案选择思科 S5730-68C-HI 型交换机作为汇聚层设备。该设备支持最大 48 个千兆接口和 4 个万兆 SPF+ 接口，还提供 2 个扩展插槽，接口丰富。其背板带宽为 758Gbps，最大扩展容量可达 7.58Tbps，能够满足公司当前及未来的网络需求，如图 2.4 所示。

图 2.4 思科 S5730-68C-HI 设备外观图

3、接入交换机

接入交换机直接面对各种终端设备，部署在各个机房，通过光纤或千兆接口连接到汇聚交换机。鉴于当前端口数量不足的情况，接入交换机必须支持最大 48 个

千兆接口和 4 个万兆 SFP+ 接口，并具备 PoE 功能。此次选择的接入层设备是思科 SF220-48-K9-CN 48 口千兆交换机。该设备具备丰富的业务特性，支持 Dos 防攻击等多种安全保护功能，同时具备强大的性能和扩展能力，能够满足公司终端设备的接入需求，如图 2.5 所示。

图 2.5 思科 SF220-48-K9-CN 设备外观图

三、网络升级改造方案设计

（一）网络架构设计

在本次网络升级改造中，首先需要对公司现有网络进行全面评估，然后针对主干网络性能进行有针对性的提升，并确保设备和链路具备冗余备份能力。鉴于公司各部门之间的业务关联较为复杂，需要通过划分 VLAN 的方式来实现部门间的网络隔离。同时，考虑到升级后的网络将承载大量高流量、高密度的信息应用，且需满足公司实际生产发展的需求，本次总体方案设计如下：

（1）设备更新替换处理

本次升级将更换部分关键网络设备，包括 2 台核心层交换机、4 台汇聚层交换机和 6 台接入层交换机。此外，还将把现有的百兆线缆升级为千兆线缆，从而全面提升网络至千兆水平。这一举措旨在从根本上解决设备老化问题，逐步降低故障率和设备超期服役的风险，进而减少网络设备的维护成本。

（2）核心网络设备的设计

核心网络设备的设计需充分考虑公司日常业务、生产和管理的网络需求。公司日常的网络通信、网络教育、语音会议、视频会议以及远程协助等应用，均需要一个高稳定、高质量的网络环境来支持。因此，核心网络设备的设计将重点保障这些关键应用的顺畅运行。

（3）汇聚网络设备的设计

汇聚层设备位于核心层与接入层之间，承担着承上启下的关键角色。它上连核心层设备，下连接入层设备，主要负责汇聚接入层的流量数据，并根据接入层的需求将数据转发至核心层设备。因此，汇聚层设备必须具备高性能和高转发速度，以确保数据传输的高效性。

（4）网络性能提升处理

通过对公司主干线路的升级、设备的更新以及相应配置的优化管理，整个主干网络将全面提升至千兆网络的运行状态。这一升级将有效解决原本多媒体业务高清化以及云业务开展时面临的性能瓶颈问题，为未来融入云计算技术做好前期技术铺

垫。

本次方案升级改造的重点在于核心层与汇聚层，这也是公司的主干网。升级更新后的主干网设备将大幅提升其整体性能，例如可将主干网链路带宽从 100M 提升至 10G，并为未来的 41G/100G 系统升级提供扩展空间。同时，这一举措将在很大程度上增强网络运行的稳定性，为公司主干网的安全及平稳运行提供有力保障。

综合考虑公司网络的实际情况以及当今社会的需求，同时兼顾未来网络扩展的能力，本次升级改造后的网络拓扑图如图 3.1 所示：

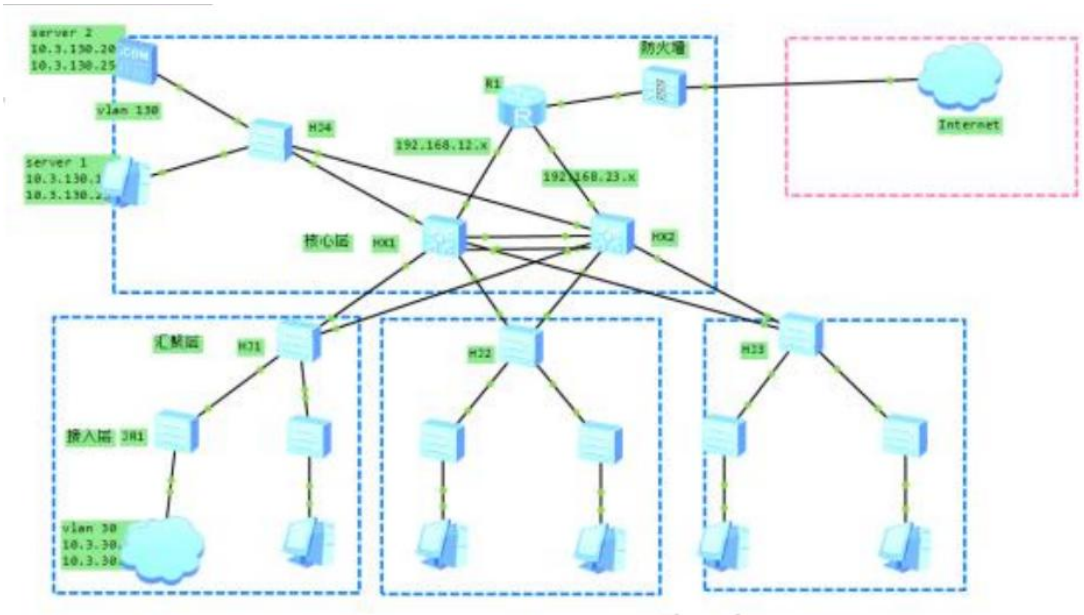

图 3.1 升级改造后拓扑图

（二）核心层设计

核心层网络作为公司网络的主干部分，是整个网络的枢纽中心，必须具备高性能、可靠性、冗余性、安全性及可管理性等特点。它负责处理公司内网、外网等各类数据流量的高速转发，保障整个公司网络的性能。核心层网络设计将采用全连接网络结构，并运用 MSTP、VRRP、链路聚合三种网络技术来实现流量负载分担以及冗余备份。同时，结合 MSTP 优化技术，加快 STP 快速收敛，减少 STP 震荡，如图 3.2 所示：

图 3.2 核心层设备连接图

（1）MSTP（多生成树协议）

MSTP 是基于 VLAN 的 STP 升级版本，全称为 Multiple Spanning Tree Protocol。它通过将一个有环路的网络修剪为一个没有环路的树形结构，避免了数据报文在环路网络中无限循环和无限转发的问题。同时，MSTP 为数据转发提供了多个冗余路径，实现了数据在转发过程中的负载分担。作为 STP 与 RSTP 的优化升级版本，MSTP 完全兼容 STP 及 RSTP，并修复了它们的缺点，具备快速收敛和负载分担的能力。

（2）VRRP（虚拟路由冗余协议）

VRRP 的全称为 Virtual Router Redundancy Protocol，它通过将多台具有路由功能的三层网络设备划分为一个 VRRP 组，形成一台具有网关功能的虚拟路由器。该虚拟路由器不仅拥有虚拟 IP 地址，还具备虚拟 MAC 地址，其功能与真实的路由器完全一致。

（3）链路聚合

链路聚合（Link Aggregation）是将两个或两个以上的物理端口加入到一个聚合组里，形成一个逻辑端口。它既可以提供流量的负载分担，又可以实现链路冗余，从而确保网络连接具有更好的可靠性。

（三）汇聚层设计

汇聚层设备位于核心层与接入层的中间位置，上连核心层设备，下连接入层设备。其主要功能是汇聚接入层的流量数据，并根据接入层的需求将数据转发给核心层设备。本次升级改造方案中，汇聚层交换机将连接两台核心交换机，实现汇聚层与核心层的链路冗余和负载分担。而汇聚层交换机与接入层交换机之间则采用单条

链路连接，如图 3.3 所示：

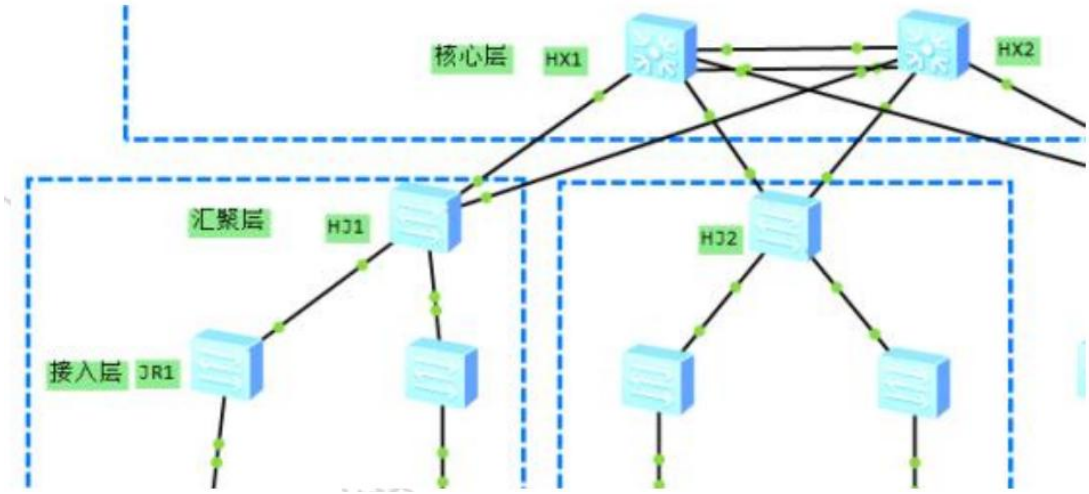

图 3.3 汇聚层设备连接图

（四）划分多区域 VLAN

随着万联科技有限公司业务的不断发展，生产业务量持续增加，接入公司网络的终端设备和 PC 电脑数量也越来越多。这导致当前公司网络端口不足，IP 地址池紧张。因此，根据公司需求设计 VLAN（虚拟局域网）划分显得尤为重要。通过划分 VLAN，可以为公司网络灵活划分多个网段、多个区域，分配给各个部门使用，从而增加部门数据的安全性，并扩充 IP 地址池。结合公司未来的生产需求，本次升级改造将为公司各个部门划分相应的 VLAN，实现 VLAN 隔离，使得特殊部门之间的数据不互通，有效提升网络管理性和数据安全性。

从交换机的原理来看，划分 VLAN 具有以下作用：

（1）防范广播风暴

当局域网产生广播风暴时，局域网内的所有主机都将受到影响，导致网络瘫痪。通过划分 VLAN，可以减少广播风暴影响的范围，防止其影响整个局域网。

（2）增强数据安全性

根据公司需求，需要将实验区域网络与其他部门网络隔离。通过划分 VLAN 技术可以实现这一目标，并减少实验数据泄露的可能性。

（3）增加接入的灵活性

通过划分 VLAN 技术，可以将公司相应部分的位置划分在一起，形成一个 VLAN。这样，不同的设备可以在不同的 VLAN 中接入使用，实现接入组网的灵活性，有效减少网络管理人员的工作量。

（4）增加设备的利用率

根据划分 VLAN 的原理，可以增加交换机端口的利用率，实现一台交换机划分多个 VLAN，使终端电脑能够接入不同网段，减少网络管理人员的配置工作量。

在本次升级方案初期，将对网络中所有接入用户进行统计，并划分相应的用户组。具体规划情况如表 3.1 所示：

表 3.1 VLAN 规划表

VLAN 号	地址段	备注
VLAN 100	10.3.100.0/24	交换机管理地址
VLAN 110	10.3.110.0/24	无线 AP 管理地址
VLAN 120	10.3.120.0/24	考勤打卡
VLAN 130	10.3.130.0/24	厂级服务器
VLAN 140	10.3.140.0/24	监控
VLAN 150	10.3.150.0/24	实验室
VLAN 160	10.3.160.0/24	外来人员
VLAN 20	10.3.20.0/24	总经办
VLAN 30	10.3.30.0/24	信息技术部
VLAN 40	10.3.40.0/24	人力资源部
VLAN 50	10.3.50.0/24	财务部
VLAN 60	10.3.60.0/24	工程部
VLAN 70	10.3.70.0/24	生产部

（五）虚拟化设计

为了满足公司生产业务需求，本次升级改造方案将核心层设备采用 VRRP 技术，并通过双链路连接汇聚层设备，从而实现核心层与汇聚层的链路冗余和负载分担。

具体来说，将两台核心交换机加入一个 VRRP 组，虚拟成一台路由器。该虚拟路由器具备虚拟 IP 地址和虚拟 MAC 地址，功能与真实路由器完全一致。VRRP 组由主核心交换机和备核心交换机组成，当主核心交换机发生宕机或线路故障时，备核心交换机将立即接手主核心交换机的工作，确保生产业务的不间断性。

此外，尽管本次升级改造方案设计的核心层设备与汇聚层设备可以实现链路冗余和负载分担，但需要搭配 MSTP 技术使用。因为双链路设计的网络容易产生环路，而 MSTP 技术可以消除环路，避免数据报文在环路网络中无限循环和无限转发。同时，MSTP 技术还为数据转发提供了多个冗余路径，实现了数据在转发过程中的负载分担。

（六）安全策略设计

（1）BFD 联动机制

BFD（双向转发检测，Bidirectional Forwarding Detection）是一种核心层设备的毫秒级链路故障检查机制，能够实现链路故障的快速切换。这一机制可以有效减少设备故障对公司生产业务的影响。

（2）DHCP 安全技术

在接入层设备中采用 DHCP Snooping 技术，可以有效防止非法 DHCP 服务器对公司网络的干扰，保障公司网络的正常运行。

（3）ACL：访问控制列表

ACL（Access Control List）主要用于数据包的访问控制。通过对流量或数据包的限制，ACL 可以对设备的访问进行控制，有效防止管理员在非法或不安全的终端设备上登录公司的网络设备，从而提高公司网络的数据安全性。

（4）STP 优化

通过设置 stp edge-port（边缘端口），为与终端连接的网络端口提供优化。这一措施可以减少 STP 的计算时间，实现网络中的快速收敛。

（5）SSH 配置

SSH（安全的远程控制协议，Security Shell）是一种加密传输数据的协议。

它为公司网络管理员在远程访问时提供安全、加密的会话，有效防止信息泄露的风险。

四、网络升级实施

（一）核心层实施

核心层的主要职责是优化骨干网络之间的数据传输，作为所有网络流量的最终承载者和汇聚点，核心层设备的性能和可靠性至关重要。在万联科技有限公司的网络架构中，核心层采用了两台思科 S7908 核心交换机，并通过链路聚合技术将它们以两条链路相连。这种设计不仅实现了链路和设备的冗余，还最大化地提升了核心交换机的性能，确保网络的高可用性和稳定性，如图 4.1 所示：

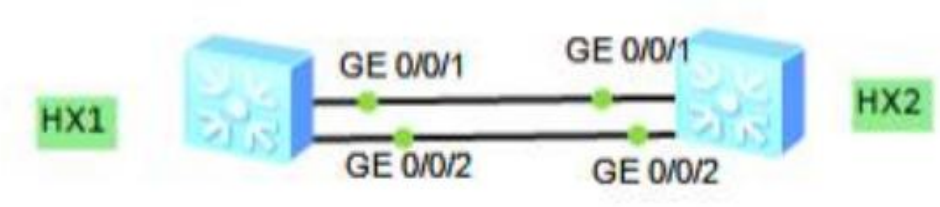

图 4.1 核心层设备 HX1 与 HX2 连接图

在进行核心层网络割接之前，需要对两台思科 S7908 交换机进行基础配置，以下是详细步骤：

（1）为了实现 HX1 和 HX2 之间的链路聚合，采用 LACP 静态模式，并将相关接口加入捆绑组 1。具体配置如下：

HX1 配置：

```
system-view  // 进入系统视图
sysname HX1  // 将设备名称更改为 HX1
interface eth-trunk 1  // 创建捆绑组 1
mode lacp-static  // 设置捆绑模式为 LACP 静态模式
trunkport gi 0/0/1  // 将接口 gi0/0/1 添加至捆绑组 1
trunkport gi 0/0/2  // 将接口 gi0/0/2 添加至捆绑组 1
```

HX2 配置：

```
system-view  // 进入系统视图
sysname HX2  // 将设备名称更改为 HX2
```

interface eth-trunk 1 // 创建捆绑组 1

mode lacp-static // 设置捆绑模式为 LACP 静态模式

trunkport gi 0/0/1 // 将接口 gi0/0/1 添加至捆绑组 1

trunkport gi 0/0/2 // 将接口 gi0/0/2 添加至捆绑组 1

完成上述配置后，需检查 eth-trunk 1 的状态，如图 4.2 和 4.3 所示。当接口状态显示为“UP”时，表明链路聚合配置成功，核心层设备之间的连接已正确建立并开始工作。通过以上配置，万联科技有限公司的核心层网络不仅具备了强大的数据传输能力，还通过冗余设计显著提升了网络的可靠性和稳定性，为公司业务的高效运行提供了坚实的基础

```
[HX1]dis int eth 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID :    1, Hash arithmetic : According to SIP-XOR-DIP,Maximal BW:
 2G, Current BW: 2G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-cccа-3310
Current system time: 2021-04-08 11:25:11-08:00
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
--------------------------------------------------
PortName                      Status      Weight
--------------------------------------------------
GigabitEthernet0/0/1          UP          1
GigabitEthernet0/0/2          UP          1
--------------------------------------------------
```

图 4.2 HX1 的 eth-trunk 1 状态

```
<HX2>dis int eth 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID :    1, Hash arithmetic : According to SIP-XOR-DIP,Maximal BW:
 2G, Current BW: 2G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-cc4a-439b
Current system time: 2021-04-11 19:45:10-08:00
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
--------------------------------------------------
PortName                      Status      Weight
--------------------------------------------------
GigabitEthernet0/0/1          UP          1
GigabitEthernet0/0/2          UP          1
--------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

图 4.3 HX2 的 eth-trunk 1 状态

（2）配置 HX1 和 HX2 的 MSTP，VLAN 10-70 在 instance 1 中，HX1 为 Primary

Root，HX2 为 Secondary Root。

VLAN 100-160 在 instance 2 中，HX1 为 Secondary Root，HX2 为 Primary Root。MSTP 的 Region name 为 DRK，revision level 为 12。

HX1 配置如下：

stp region-configuration　//进入 MSTP 配置界面

region-name DRK　//配置 MSTP 域名为 DRK

revision-level 1　//配置修订号为 1

instance 1 vlan 10 to 70　//生成树实例 1 映射 VLAN10-70

instance 2 vlan 100 to 160　//生成树实例 2 映射 VLAN100-160

active region-configuration　//激活 MSTP 配置

stp instance 1 root primary　//在实例 1 中设备作为主根桥

stp instance 2 root secondary　//在实例 2 中设备作为备份根桥

HX2 配置如下：

stp region-configuration　//进入 MSTP 配置界面

region-name DRK　//配置 MSTP 域名为 DRK

revision-level 1　//配置修订号为 1

instance 1 vlan 10 to 70　//生成树实例 1 映射 VLAN10-70

instance 2 vlan 100 to 160　//生成树实例 2 映射 VLAN100-160

active region-configuration　//激活 MSTP 配置

stp instance 1 root secondary　//在实例 1 中设备作为备份根桥

stp instance 2 root primary　//在实例 2 中设备作为主根桥

（3）核心层通过 VRRP 协议，实现冗余和负载分担。

HX1 配置如下：

interface vlanif 20　//创建 VLANIF 20

ip address 10.3.20.1 255.255.255.0　//配置 IP 和掩码

vrrp vrid 2 virtual-ip 10.3.20.254　//在 VRID 2 备份组中的虚拟网关地址

vrrp vrid 2 priority 105　//在 VRID 2 备份组优先级 105，保证 master

interface vlanif 30　//创建 VLANIF 30

ip address 10.3.30.1 255.255.255.0　//配置 IP 和掩码

vrrp vrid 3 virtual-ip 10.3.30.254　//在 VRID 3 备份组中的虚拟网关地址

vrrp vrid 3 priority 105　//在 VRID 3 备份组优先级 105，保证 master

…

…

interface vlanif 160　//创建 VLANIF 160

ip address 10.3.160.1 255.255.255.0　//配置 IP 和掩码

vrrp vrid 160 virtual-ip 10.3.160.254　//在 VRID 160 备份组中的虚拟网关地址

vrrp vrid 160 priority 105　//在 VRID 160 备份组优先级 105，保证 master

HX2 配置如下：

interface vlanif 20　//创建 VLANIF 20

ip address 10.3.20.2 255.255.255.0　//配置 IP 地址，掩码

vrrp vrid 2 virtual-ip 10.3.20.254　//在 VRID 2 备份组中处 backup

interface vlanif 30

ip address 10.3.30.2 255.255.255.0　//配置 IP 地址、子网掩码

vrrp vrid 3 virtual-ip 10.3.30.254　//在 VRID 3 备份组中处 backup

…

…

interface vlanif 160　//创建 VLANIF 160

ip address 10.3.160.2 255.255.255.0　//配置 IP 地址、子网掩码

vrrp vrid 160 virtual-ip 10.3.160.254　//在 VRID 160 备份组中处 backup

（4）HX1 和 HX2 路由配置

HX1 配置如下：

ospf 1　// 启动 OSPF 进程 1

area 0.0.0.0　// 创建 OSPF 区域 0

network 10.3.20.0 0.0.0.255　// 声明 VLAN 20 的网络段

network 10.3.30.0 0.0.0.255　// 声明 VLAN 30 的网络段

network 10.3.40.0 0.0.0.255　// 声明 VLAN 40 的网络段

// 重复上述步骤，声明 VLAN 50 到 VLAN 160 的网络段

HX2 配置如下：

ospf 1 // 启动 OSPF 进程 1

area 0.0.0.0 // 创建 OSPF 区域 0

network 10.3.20.0 0.0.0.255 // 声明 VLAN 20 的网络段

network 10.3.30.0 0.0.0.255 // 声明 VLAN 30 的网络段

// 重复上述步骤，声明 VLAN 40 到 VLAN 160 的网络段

network 10.3.160.0 0.0.0.255 //宣告外人人员地址

通过 OSPF 配置，HX1 和 HX2 能够实时交换路由信息，确保网络中的数据包能够通过最短路径进行传输，提高了网络的效率和可靠性。

通过对 HX1 和 HX2 的 MSTP、VRRP 和 OSPF 配置，万联科技有限公司的核心层网络不仅实现了链路和设备的冗余，还优化了流量分配和路由选择。这些配置确保了网络的高可用性、稳定性和高效性，为公司业务的持续发展提供了坚实的基础。

（二）汇聚层实施

汇聚层是楼群或小区的信息汇聚点,是连接接入层和核心层的网络设备,为接入层提供数据的汇聚、传输、管理、分发处理。汇聚层为接入层提供基于策略的连接，如地址合并，协议过滤、路由服务、认证管理等。万联科技有限公司汇聚层是使用思科 S5730 交换机作为汇聚层设备，并与核心层的两台核心交换机相连接，即使一条链路故障，还可以走另一条链路，这就是链路冗余。还可以为链路负载分担，如图 4.4 所示：

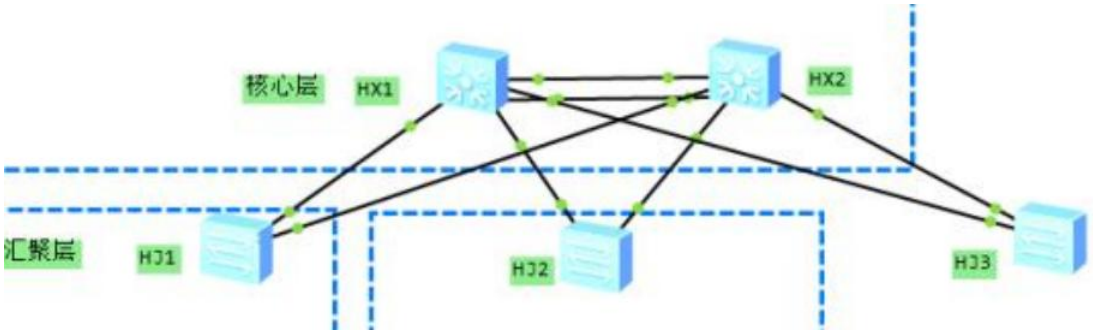

图 4.4 汇聚层设备连接图

（1）首先进行汇聚层设备（HJ1、HJ2、HJ3、HJ4）链路聚合配置，如下：

HJ1 配置如下：

system-view　//进入系统视图

sysname HJ1　//更改设备名称为 HX1

interface eth-trunk 1　//创建捆绑组 1

mode lacp-static　//设置模式为 lacp-static

trunkport gi 0/0/1　//将接口 gi 0/0/1 加入捆绑组 1

trunkport gi 0/0/2　//将接口 gi 0/0/2 加入捆绑组 1

HJ2 配置如下：

system-view　//进入系统视图

sysname HJ2　//更改设备名称为 HX1

interface eth-trunk 1　//创建捆绑组 1

mode lacp-static　//设置模式为 lacp-static

trunkport gi 0/0/1　//将接口 gi 0/0/1 加入捆绑组 1

trunkport gi 0/0/2　//将接口 gi 0/0/2 加入捆绑组 1

（2）MSTP 配置，HJ1、HJ2 如下：

stp region-configuration　//进入 MSTP 配置界面

region-name DRK　//配置 MSTP 域名为 DRK

revision-level 1　//配置修订号为 1

instance 1 vlan 10 to 70　//生成树实例 1 映射 VLAN10-70

instance 2 vlan 100 to 160　//生成树实例 2 映射 VLAN100-160

active region-configuration　//激活 MSTP 配置

（3）VLAN 配置，如下：

vlan batch 20 30 40……　//创建 VLAN 20、30、40……

interface Eth-Trunk 1　//进入聚合接口 1

port link-type trunk　//将接口类型定义为 trunk

port trunk allow-pass vlan all　//允许所有接口通过

interface Ethernet 0/0/2　//进入 e 0/0/2 接口

port link-type trunk　//将接口类型定义为 trunk

port trunk allow-pass vlan all　//定义 trunk 允许 vlan 通过

（三）接入层实施

接入层常利用光纤、双绞线、同轴电缆、无线接入技术等传输介质，实现与用户连接，并进行业务和带宽的分配。接入层的目的是允许终端用户连接到网络，因此接入层交换机具有低成本和高端口密度特性。如图 4.5 所示，万联科技有限公司接入层交换机替换为两台思科 S5720 交换机，传输速率最高支持 1000Mbps，只要与汇聚层的接口配置为干道即可。对于人员流量多的部门，可以安装无线 AP。

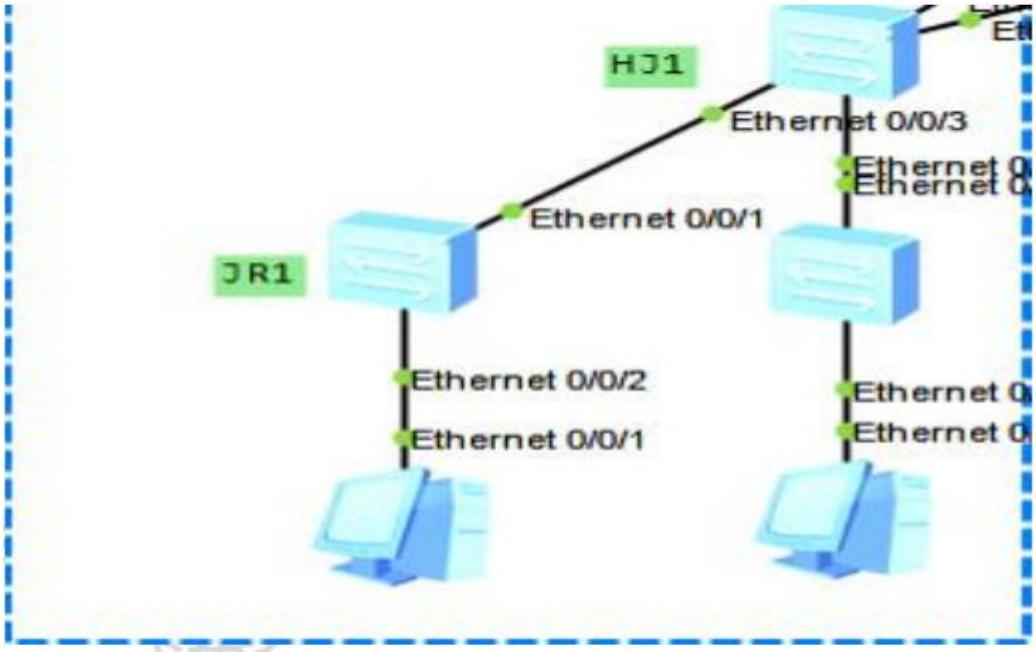

图 4.5 接入层设备连接图

接入层交换机的配置，如下：

vlan batch 20 30 40……　//创建 VLAN 20、30、40……

interface Ethernet 0/0/1　//进入 e 0/0/1 接口

port link-type trunk　//将接口类型定义为 trunk

port trunk allow-pass vlan all　//定义 trunk 允许 vlan 通过

（四）安全策略实施

入侵检测就是对入侵行为的检测,通过收集和分析计算机网络或计算机系统中若干关键点的信息,检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象,而蜜罐的目的在于吸引攻击者、然后记录下一举一动的计算机系统,攻击者入侵后,可以随时了解其针对服务器发出的最新的攻击和漏洞,这样系统就可以及时、有针对性的防范攻击和修复漏洞。

（1）HX1 和 HX2 的 BFD 联动配置，如下：

HX1 BFD 配置：

bfd　//全局使能 bfd

bfd BFD bind peer-ip 192.168.12.1 source-ip 192.168.12.2 auto

　//配置 bfd 组

commit　//确认提交

interface vlanif 20　//进入 vlanif 20 接口

vrrp vrid 2 track interface GigabitEthernet 0/0/1

vrrp vrid 2 track bfd-session session-name BFD

interface vlanif 30　//进入 vlanif 30 接口

vrrp vrid 3 track interface GigabitEthernet 0/0/1

　//配置 VRRP 监视接口 g 0/0/1

vrrp vrid 3 track bfd-session session-name BFD

　//配置 VRRP 与 BFD 联动

……

HX2 BFD 配置：

bfd　//全局使能 bfd

bfd bfd bind peer-ip 192.168.23.1 source-ip 192.168.23.2 auto

　//配置 bfd 组

commit　//确认提交

interface vlanif 4　//进入 vlanif 4 接口

vrrp vrid 4 track interface GigabitEthernet 0/0/4

//配置 VRRP 监视接口 g 0/0/4

vrrp vrid 4 track bfd-session session-name bfd

//配置 VRRP 与 BFD 联动

interface vlanif 5 //进入 vlanif 5 接口

vrrp vrid 5 track interface GigabitEthernet 0/0/4

//配置 VRRP 监视接口 g 0/0/4

vrrp vrid 5 track bfd-session session-name bfd

//配置 VRRP 与 BFD 联动

R1 BFD 配置：

bfd //全局使能 bfd

bfd BFD bind peer-ip 192.168.12.2 source-ip 192.168.12.1 auto

//配置 bfd 组

commit //确认提交

bfd bfd bind peer-ip 192.168.23.2 source-ip 192.168.23.1 auto

//配置 bfd 组

commit //确认提交

（2）DHCP 安全技术，如下：

接入层交换机 JR1、JR2、JR3……

dhcp enable //使能 DHCP 服务

dhcp snooping enable //使能 DHCP Snooping 服务

vlan X //进入 vlan X

dhcp snooping enable //使能 DHCP Snooping 服务

int e 0/0/1 //进入 e 0/0/1 接口

dhcp snooping trusted //设置为 DHCP 信任接口

（3）ACL 配置如下

acl 2001 //创建 ACL 2001

rule 5 permit source 10.3.30.0 0.0.0.255 //配置规则 5

rule 10 deny soure 10.3.0.0 0.0.255.255　//配置规则 10

user-interface vty 0 4　//进入虚拟终端

acl 2001 inbound　//在出方向调用 ACL 2001

authentication-mode aaa　//AAA 认证

（4）STP 优化配置

接用户和服务器的接口需要配置边缘端口

int e 0/0/x　//进入 e 0/0/x 接口

stp edge-port enable　//使能边缘端口

HX1、HX2 上联路由器接口禁用 STP

int gi 0/0/x　//进入 gi 0/0/x 接口

stp disable　//停用 stp 服务

给捆绑接口配置静态的 cost 开销

int eth-trunk x　//进入聚合端口组

stp instance 1 cost 10000　//设置实例 1 开销为 10000

（5）SSH 配置如下：

rsa local-key-pair create　//创建密钥对

user-interface vty 0 4　//配置 VTY 用户界面

authentication-mode aaa　//使用 aaa 里面的用户名和密码进行验

protocol inbound ssh

aaa　//创建 SSH 用户名密码

local-user drk password cipher drk123　//配置用户名 drk，密码 drk123

local-user drk privilege level 3　//配置用户名 drk 权限级别 3 级

local-user drk service-type ssh　//定义该账户服务类型

ssh user drk authentication-type password　//密码验证方式

ssh user drk service-type stelent　//服务类型为 stelnet

stelnet server enable　//使能 SSH 服务

五、改造后的网络测试

（一）测试目的

本次网络升级改造旨在实现公司网络架构的全面升级，从旧有架构迈向新的高效架构。为确保升级改造达到预期目标，使用专业测试工具对新网络及设备进行全面测试至关重要。测试内容涵盖网络冗余性、可用性、负载能力等方面，通过测试结果评估网络升级改造方案是否满足预期要求。

（二）测试内容

新网络运行测试的主要内容如下：

（1）网络连通性测试

通过多台电脑终端分别连接接入交换机、汇聚交换机以及核心交换机，并测试与互联网的连通性。确保网络设备之间的通信顺畅无阻。

（2）设备冗余性测试

在核心交换机正常运行时，模拟故障场景，例如关闭 Master 核心交换机或拔掉其网络线缆，观察 Backup 核心交换机是否能迅速切换为 Master 并接管工作。通过持续的 ping 测试监测网络丢包情况，验证设备冗余机制的有效性。

（3）安全策略测试

利用多台终端电脑与网络设备进行交互，测试安全策略是否按预期生效。借助抓包软件 Wireshark 分析数据包，验证访问控制列表（ACL）是否正常工作，确保网络流量符合安全策略要求。

（三）测试过程

（1）VRRP 状态及冗余测试

使用 display vrrp brief 命令查看两台核心交换机的当前 VRRP 状态。如图 5.1 和 5.2 所示，核心交换机 1 的状态为 Master，核心交换机 2 的状态为

Backup。

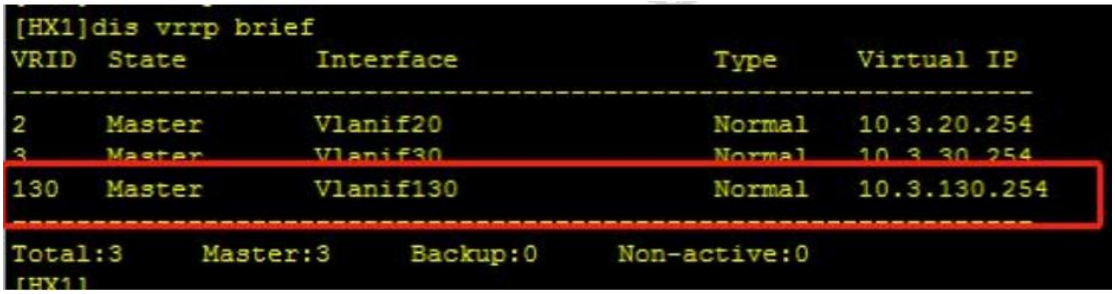

图 5.1 核心交换机 1 测试前的 VRRP 状态

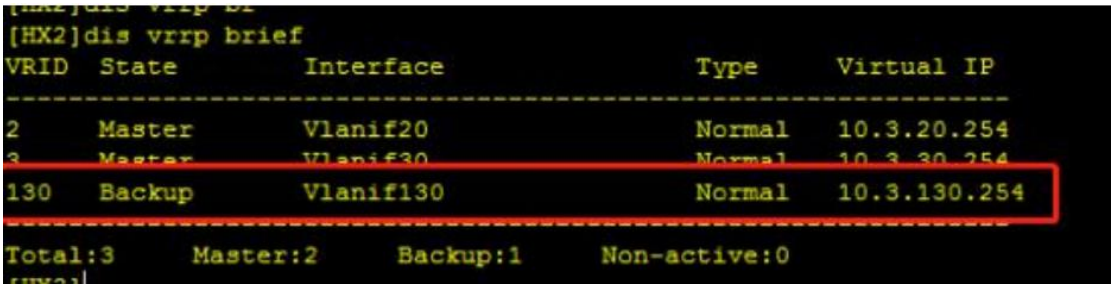

图 5.2 核心交换机 2 测试前的 VRRP 状态

多台终端电脑同时 ping 两台核心交换机的虚拟 IP 地址，验证网络连通性。如图 5.3 所示，网络连通正常：

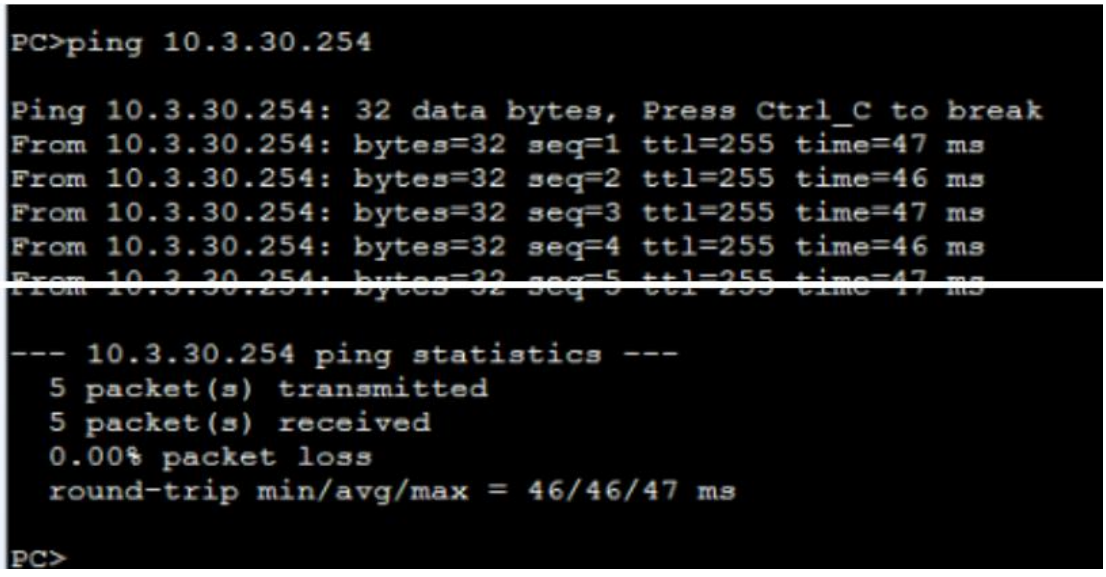

图 5.3 网络切换前使用 ping 测试

一台终端电脑持续 ping 虚拟网关 IP 地址 10.3.30.254，随后关闭核心交换机 1 或拔掉其网线，观察终端电脑 ping 窗口的信息状态。如图 5.4 所示，出现三个或以下丢包现象可视为正常，表明网络已从核心交换机 1 快速切换到核心交

换机 2，用户几乎无感知。

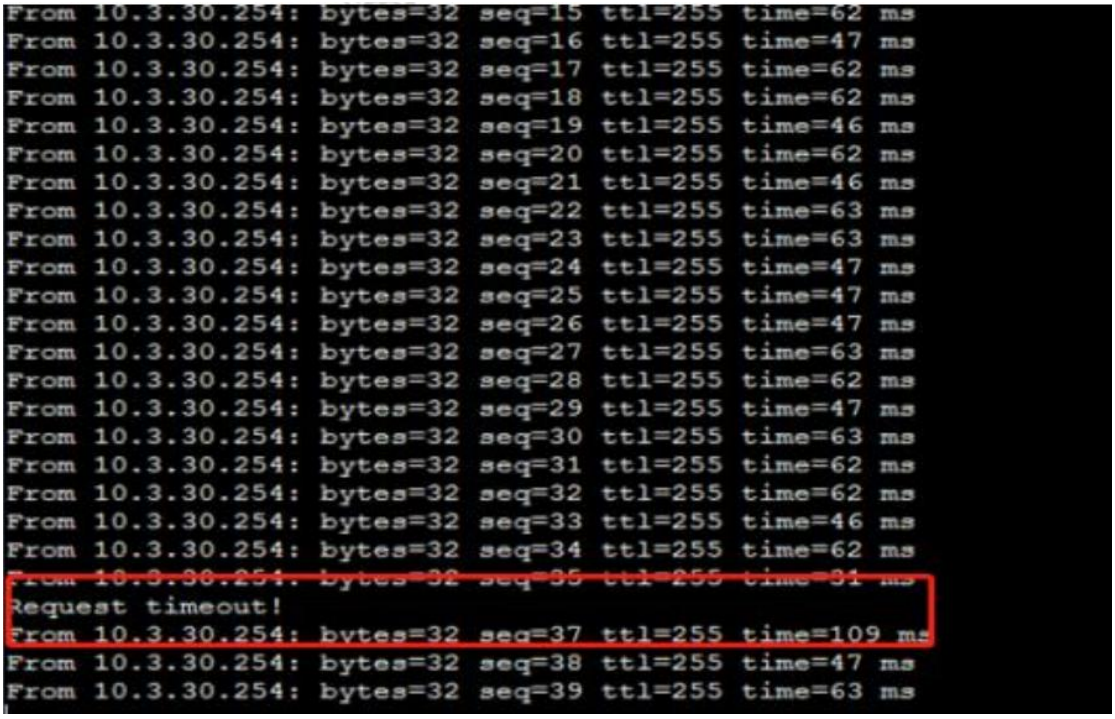

图 5.4 网络切换后 ping 测试

重新启动核心交换机 1 或插回网线，再次使用 display vrrp brief 命令查看两台核心交换机的 VRRP 状态。如图 5.5 所示，核心交换机 1 的状态应为 Backup，核心交换机 2 的状态应为 Master。

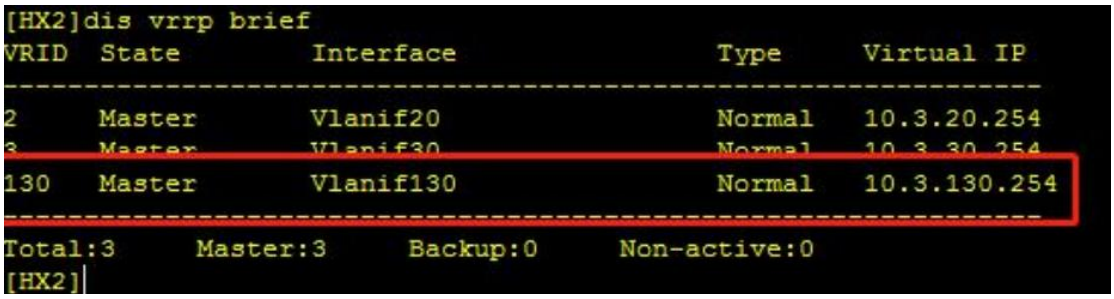

图 5.5 核心交换机 2 测试后的 VRRP 状态

测试结果表明，网络切换成功，切换过程中仅丢失一个数据包，未对生产业务造成影响。

（2） 链路聚合状态及冗余测试

使用 display interface eth-trunk 1 命令查看两台核心交换机当前聚合口状态。如图 5.6 和 5.7 所示，核心交换机 1 上的 gi 0/0/1 和 gi 0/0/2 状态

为 UP，核心交换机 2 上的 gi 0/0/1 和 gi 0/0/2 状态也为 UP。

```
[HX1]display interface Eth-Trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID :    1, Hash arithmetic : According to SIP-XOR-DIP,Maximal BW:
 2G, Current BW: 2G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-ccca-3310
Current system time: 2021-04-11 21:58:31-08:00
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
--------------------------------------------------
PortName                      Status      Weight
--------------------------------------------------
GigabitEthernet0/0/1          UP          1
GigabitEthernet0/0/2          UP          1
--------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

图 5.6 核心交换机 1 测试前的聚合口状态

```
<HX2>dis int eth 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID :    1, Hash arithmetic : According to SIP-XOR-DIP,Maximal BW:
 2G, Current BW: 2G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-cc4a-439b
Current system time: 2021-04-11 22:00:53-08:00
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
--------------------------------------------------
PortName                      Status      Weight
--------------------------------------------------
GigabitEthernet0/0/1          UP          1
GigabitEthernet0/0/2          UP          1
--------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

图 5.7 核心交换机 2 测试前的聚合口状态

多台终端电脑同时 ping 核心交换机的虚拟 IP 地址 10.3.30.254，验证网络连通性。如图 5.8 所示，网络连通正常：

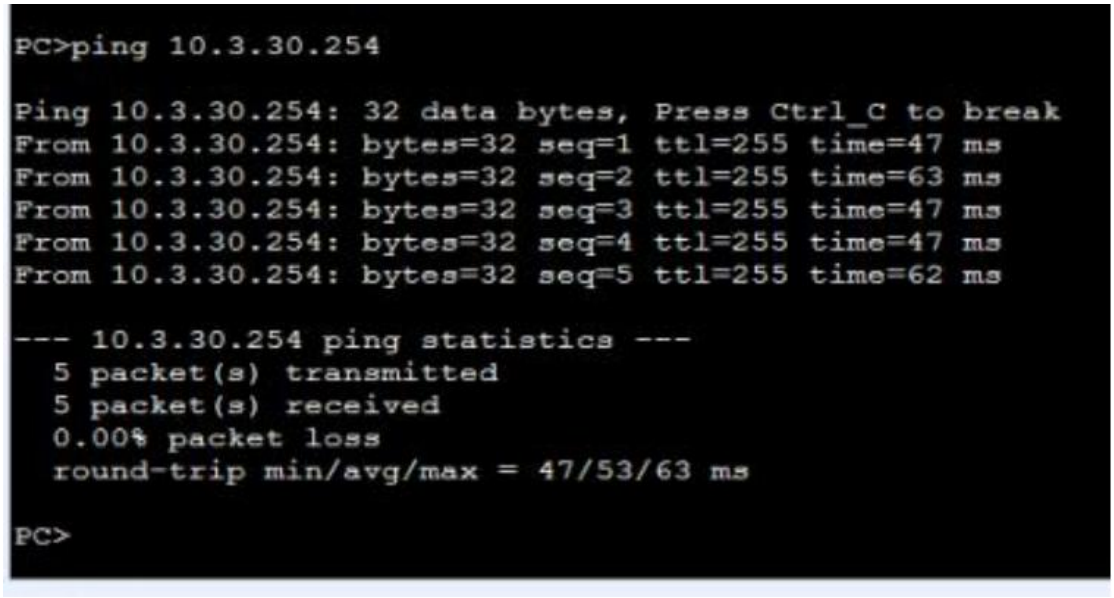

图 5.8　ping 核心交换机的虚拟 IP 测试

一台终端电脑持续 ping 虚拟网关 IP 地址 10.3.30.254，随后拔掉核心交换机聚合组的一条聚合链路，观察终端电脑 ping 窗口的信息状态。如图 5.9 所示，测试结果显示网络稳定，未出现丢包现象，验证了核心交换机聚合链路技术的可靠性。

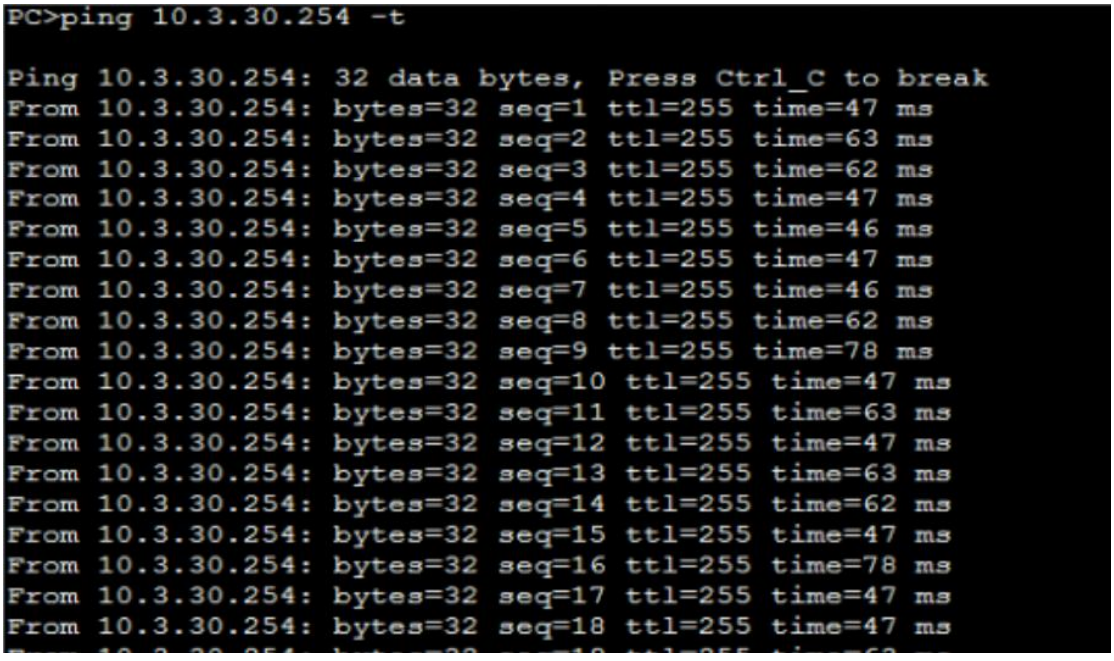

图 5.9 终端电脑 ping 测试

（3）安全策略及 ACL 测试

使用一台位于 10.3.30.0 网段的电脑终端尝试通过 telnet 登录交换机。成功登录并出现密码输入提示框，表明 ACL 规则生效，允许该网段的设备访问交换机。如图 5.13 所示：

使用抓包软件 Wireshark 对 telnet 登录交换机的过程进行抓包分析。如图 5.14 所示，分析结果显示数据包经过加密处理，进一步验证了安全策略的有效性。

```
PC>ping 10.3.1.1

Ping 10.3.1.1: 32 data bytes, Press Ctrl_C to break
From 10.3.1.1: bytes=32 seq=1 ttl=255 time=47 ms
From 10.3.1.1: bytes=32 seq=2 ttl=255 time=47 ms
From 10.3.1.1: bytes=32 seq=3 ttl=255 time=62 ms
From 10.3.1.1: bytes=32 seq=4 ttl=255 time=47 ms
From 10.3.1.1: bytes=32 seq=5 ttl=255 time=63 ms

--- 10.3.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 47/53/63 ms

PC>
```

图 5.10 安全登陆 ping 测试

查看该交换机的访问控制列表配置，如图 5.11 所示：

```
[HX1]
[HX1]dis acl 2000
Basic ACL 2000, 2 rules
Acl's step is 5
 rule 5 permit source 10.3.30.0 0.0.0.255
 rule 10 deny source 10.3.0.0 0.0.255.255

[HX1]
```

图 5.11 交换机 ACL 配置

任意使用一台终端电脑且不在 10.3.30.0 的网段去尝试 telnet 登陆交换机，会显示连接失败，说明没有权限登陆交换机，如图 5.12 所示：

图 5.12 非指定地址登陆测试

任意使用一台电脑终端且在 10.3.30.0 的网段去尝试登陆 telnet 交换机，会跳到输入密码的提示框，说明能成功登录到交换机上，并且验证说明 ACL 的规则是可行，如图 5.13 所示：

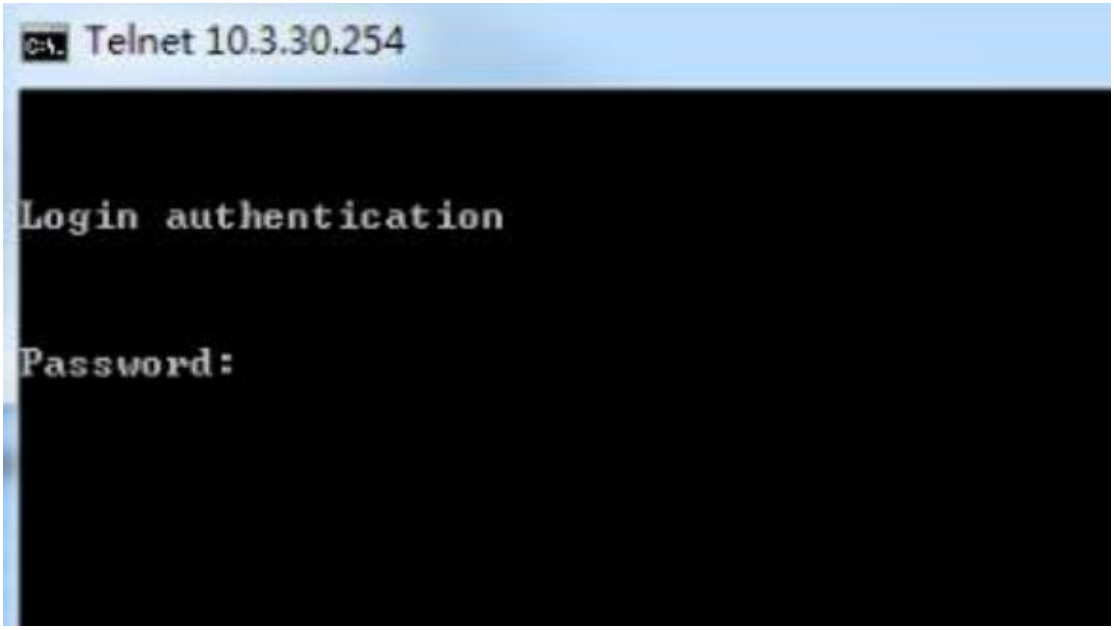

图 5.13 指定地址登陆测试

（4）使用抓包软件 Wireshark[9]对 telnet 登录交换机的过程进行抓包分析，如图 5.14 所示：

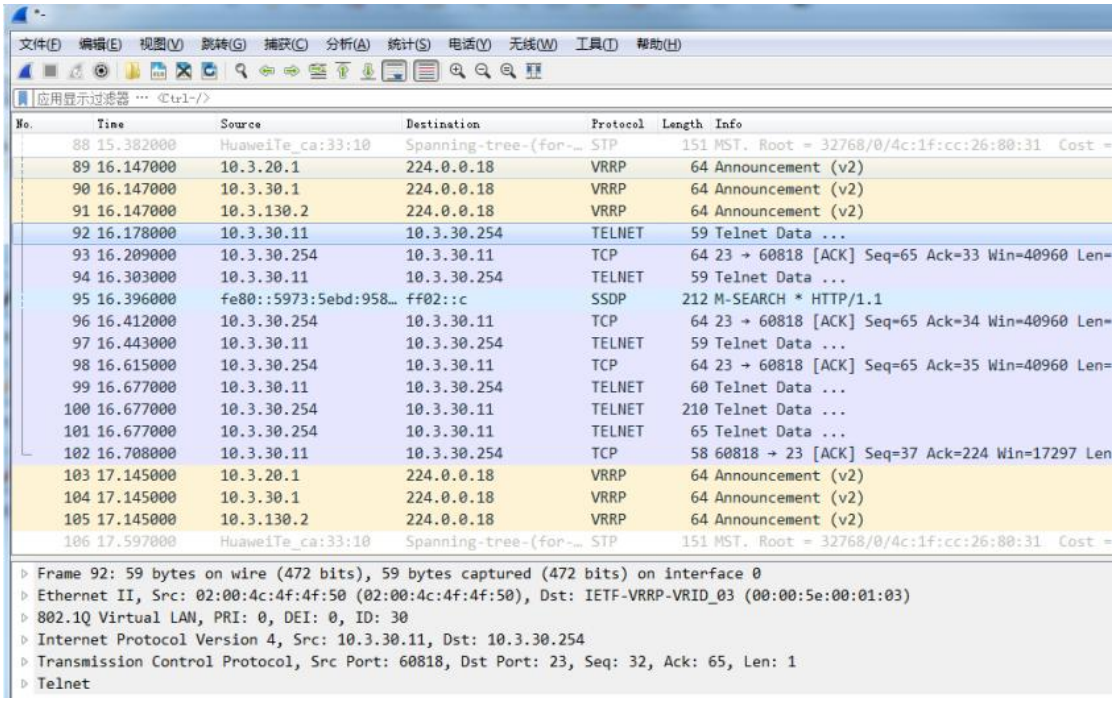

图 5.14　Wireshark 抓包结果

（四）测试结果

本次测试涵盖网络连通性测试、设备冗余性测试和安全策略测试。网络连通性测试结果表明，多台终端电脑对网络的测试显示网络连通正常。设备冗余性测试通过两种方式验证：

关闭核心设备或拔掉线缆，测试结果显示网络未出现高延迟或长时间中断，设备冗余机制有效。

拔掉核心设备的线缆，测试链路冗余，结果显示网络稳定运行，未出现丢包现象，链路冗余机制可靠。

安全策略测试通过多台终端电脑对网络设备的测试，结果证明 ACL 规则生效，且抓包软件 Wireshark 分析显示数据包经过加密处理。

随着万联科技有限公司新网络施工完成并经过一系列测试，根据测试结果，网络的冗余性、可靠性基本达到方案预期标准，能够满足公司的生产业务需求。后续需持续监控网络使用状况，如有问题及时优化，确保网络始终保持最佳状态。

。

总 结

通过本次网络升级改造方案，万联科技有限公司成功构建了一个高性能、高稳定性的网络环境，为公司的生产与业务运营提供了坚实的支撑。该方案紧密结合公司当前的业务需求与网络技术发展趋势，不仅满足了日常业务的网络需求，还为未来的扩展预留了充足的空间。

本次方案的主要工作有以下几个方面：

（1）网络现状分析与研究

对公司现有网络状况进行了全面的评估与分析，深入研究了大量网络技术文献和相关资料，了解了当前中国网络技术的发展趋势。结合公司的生产与业务需求，提出了一套综合的网络升级改造方案。该方案涵盖了对现有网络架构的重新设计，对超期服役的网络设备和链路进行更新替换，以及针对网络安全需求设计的安全策略。

（2）核心层设备升级

核心层作为网络的核心枢纽，其稳定性与性能直接影响到整个网络的运行。为此，采用两台思科 S7908 核心交换机，并通过链路聚合技术实现链路冗余与负载分担，确保生产业务的网络不间断运行。同时，结合网络虚拟化技术，进一步提升网络的灵活性与扩展性。

（3）汇聚层设备升级

汇聚层设备选用思科 S5730-68C-HI 敏捷型汇聚交换机，与两台核心交换机相连。通过多生成树协议（MSTP）实现链路备份，确保网络的高可靠性和冗余性。这种设计不仅提升了网络的稳定性，还为未来的业务扩展提供了坚实的基础。

（4）VLAN 灵活划分

根据公司不同部门、生产与业务需求，对网络进行了灵活的 VLAN 划分，创建了多个独立的网络区域。通过 VLAN 隔离，确保特殊部门之间的数据不互通，有效提升了网络管理的便捷性和数据的安全性。这种划分方式不仅优化了网络资源的分配，还增强了网络的整体安全性。

（5）多层次安全策略设计

针对公司的业务特性，设计并实施了多项安全策略，包括双向转发检查（BFD）、DHCP 安全技术、访问控制列表（ACL）、STP 优化以及 SSH 配置。这些策略从不同层面增强了网络的安全性，确保了公司业务生产数据的有效保护。通过这些措施，网络运维管理更加高效，数据传输更加安全可靠。

本次网络升级改造方案的成功实施，不仅为万联科技有限公司提供了高性能、高稳定性的网络环境，还为公司的未来发展奠定了坚实的基础。通过全面的网络优化与安全策略部署，公司网络的冗余性、可靠性和安全性得到了显著提升，为公司的生产与业务运营提供了有力保障。

参考资料

[1]曹吉龙.计算机网络的可靠性优化[J].电子世界,2024(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,2023.

[4]黄允凯,谈英姿.深入浅出 NetLinx 网络架构[M].机械工业出版社,2024.03.

[5]李琦.宜家酒店网络设计方案[J].湖南开放大学,2023.07.

[6]胡启龙.嘉禾职业中专网络规划方案[J].湖南开放大学,2022.04.

[7]张威龙.龙门中学校园网实施方案[J].湖南开放大学,2022.12.

[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,2022.11.

[9]唐勇.天启网络科技企业网络设计方案[J].湖南开放大学,2022.08.

[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,2022.08.