

目 录

1 项目概括	1
1.1 公司介绍	1
1.2 项目背景	1
1.3 项目需求	2
2 网络架构	2
2.1 网络总拓扑	2
2.2 设计原则	3
2.3 项目需求	4
2.4 IP 规划	4
3 网络技术选型	5
3.1 VLAN	5
3.2 NAT	5
3.3 ACL	6
3.4 OSPF	6
3.5 VRRP	6
3.6 TELNET	6
4 设备选型	7
4.1 设备选型	7
4.2 三层交换机选型	7
4.2 出口路由器选型	7
4.3 接入交换机选型	8
4.4 服务器选型	9
4.5 汇聚层交换机选型	9
5. 设备配置	10
5.1 VLAN Trunk	10
5.2 VLANIF 配置	14
5.3 DHCP 配置	15

5.4 OSPF 配置	15
5.5 NAT 配置	18
5.6 ACL 配置	18
5.6Telnet 远程管理配置	19
6 网络项目测试	20
6.1 各部门相互访问	20
6.6 分部互相访问	21
6.7 内网服务器访问	22
6.8 Telnet 远程管理测试	22
7 网络性能调优	23
7.1 OSPF 优化	23
7.2 VLAN 优化	24
8 设计小结	25
参考资料	26

京港一号公司网络规划与设计方案

1 项目概括

1.1 公司介绍

京港一号有限公司（以下简称京港一号公司）成立于 1999 年，是一家专注于运动产品和服装产品研究、开发、生产及销售的高科技企业，总部及研发基地设立于风景秀丽的桃园工业园，并在全国各地设有分支机构。公司技术和研发实力雄厚，被政府认定为“高新技术企业”。

公司自成立以来，始终坚持以人才为本、诚信立业的经营原则，荟萃业界精英，将国外先进的信息技术、管理方法及企业经验与国内企业的具体实际相结合，为企业供给全方位的解决方案，帮忙企业提高管理水平和生产本事，使企业在激烈的市场竞争中始终坚持竞争力，实现企业快速、稳定地发展。

公司人才结构合理，总部和分部均有研发部、市场部、财务部等部门，现在要求进行网络规划与设计，实现分部和总部能够进行网络连通。同时考虑为了数据安全是否应用 VPN，DNS 等技术。拥有多名博士作为主要的技术骨干，具有硕士、学士高中级技术职称的员工达 800 多人。为了开发出真正适合企业需求的运动产品，紧密跟踪运动健身产品方面的技术和行业发展特点，不断优化设计、材料款式，令用户得到最优质的服务和最好的使用体验。

1.2 项目背景

随着现代科学技术和互联网的迅猛发展,以计算机和通讯技术为基础的管理系统正处于高速发展的时期。同时,伴随着经济文化水平的显著提高,人们对生活质量的要求也在不断提升,对工作的环境以及要求也日益提高。在推动信息化建设,并保证将来可以扩展骨干网络节点为用户提供高速信息接入。并实现网络办公、资源共享等各种应用。利用现代信息技术从事办公管理、产品研究等工作。最终能通过园区网络实现教学管理高效、网络资源共享不间断的服务,方便对网络中所有设备和应用进行有效的实时控制和管理。园区内进行办公的人们之间需要相互的通信,同时在相互通信的过程中又能确保信息通畅与保密,于是对此园区的一个网络规划与设计应运而生。

公司下总部和分部均有研发部、市场部、财务部等部门,现在要求进行网

络规划与设计，实现分部和总部能够进行网络连通。同时考虑为了数据安全是否应用 VPN，DNS 等技术。各部门间为提高办公效率，促进信息交流，适应现代化办公的要求，需要组建一个完善的企业内部网。通过对园区网络的分析，从性能和价值上满足园区网络的需求，然后对企业园区网络进行划分 VLAN、设置管理域等配置，不断的优化企业的网络，从而达到企业安全、快速访问网络资源的目的。

1.3 项目需求

根据客户要求，在网络设计要采用成熟的网络技术，同时也要务必保证网络的性价比、可靠性、安全性、实用性等等。

满足服务效率、服务质量、网络吞吐率、网络响应时间、数据传输速度、资源利用率、可靠性、性价比等；实现园区内外网对 Internet 的高速、安全访问。通过数据链路冗余备份技术实现网络的稳定可靠性。要能达到低负载、高带宽、最简单、最有效要求，并实现资源共享和高效率传输。确保物理层、数据链路层、网络层稳定、可靠。确保整个园区资源的安全。

公司总部和分部之间的部门能够相互访问，公司内部有自己的服务器供各部门访问，同时配备专门的财务服务器单独供财务部门使用。公司各部门通过运营商联系外网服务器进行上网，分部可以采用单臂路由进行简单设计，外网用户可以通过内网服务器的端口映射从而访问公司服务器，但是不能访问公司各部门。

2 网络架构

2.1 网络总拓扑

公司网络采用三层结构设计，分为核心层、汇聚层、接入层。总部设立四个部门：安全部、财务部、市场部、研发部。采用三层架构，交换机之间是 Trunk 通路设置以便于不同 VLAN 通信，安全部门用路由器进行模拟。总部设立两个内部服务器：财务服务器和内网服务器，其中财务服务器只允许财务部访问，其他部门不允许访问，各部门都可以访问内网服务器。分部设立三个部门：市场部、研发部、财务部。采用单臂路由配置，分部各部门可以相互访问也可以与总部各部门相互访问，分部同样可以访问内网服务器。外网服务器和客户端都建立在运营商路由器上，通过内网出口路由使总部和分部都可以访问。具体拓扑主要如图 1 所示。

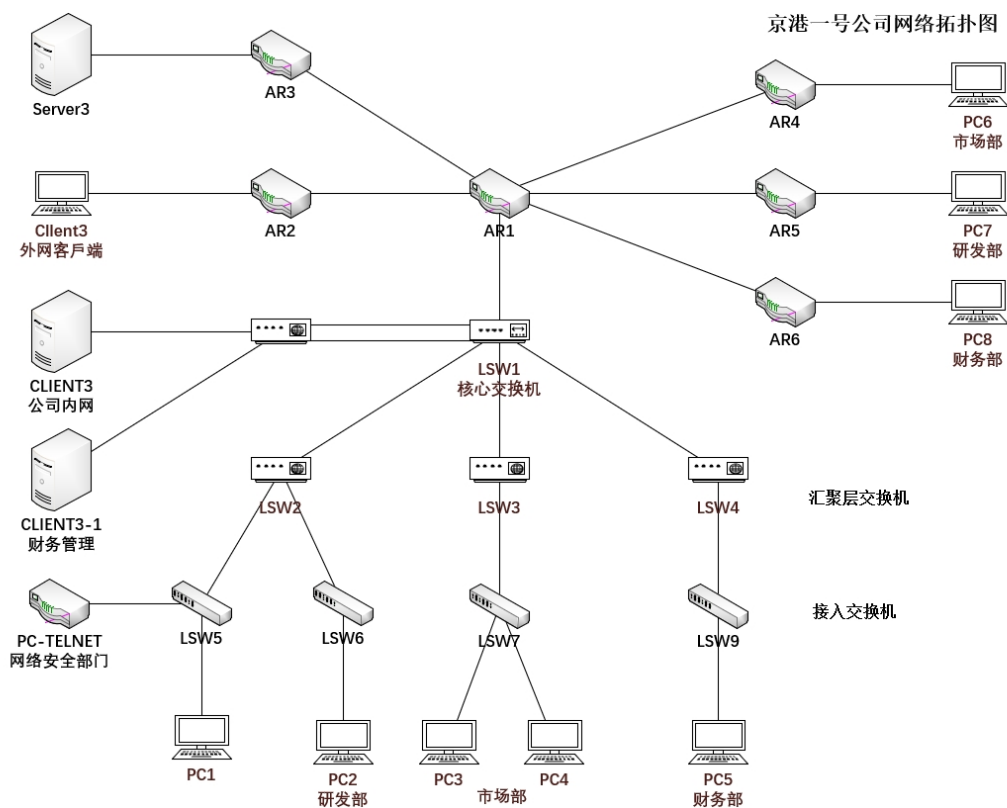


图1 京港一号公司拓扑图

2.2 设计原则

(1) 安全性

网络系统的安全性可以体现在物理安全和虚拟网络安全上，物理安全要保障网络设备存放的安全性，比如服务器的位置不能让非企业人员知晓，设备周围的物理环境也需要人工调整避免物理侵蚀，虚拟网络安全就需要我们设置服务器密码等加密操作了，比如加上企业防火墙。

(2) 先进性

在对企业网络设备选择时要紧跟时代发展，随着时代发展，网络设备也都在不断的更新换代，在选择企业网络设备时要考虑到设备的冗余性和可兼容性，要具有先进的眼光来布置网络设备，减少后期更换设备时的财政支出。

(3) 可靠性

一般的中型和大型企业都非常注重网络运行的可靠性，往往网络动荡会导致公司信息系统的瘫痪和负面形象的传播，给维修和安全维护人员带来很大的挑战，同时也大大增加了企业的财务支出费用，因此，在对企业进行网络设计时，我们首先要考虑的就是网络系统的可靠性，保证系统可以长时间的相对稳定、可靠的运行，并保证系统访问的安全性，防止非法用户非法访问。设计的

网络系统要有容错性，运行过程中难免出现设备故障，这要求网络系统要有良好的备份，避免给公司造成不可逆转的不良影响。

2.3 项目需求

随着网络时代的快速发展，越来越多的设备厂商应运而生，不同设备厂商有着各自不同的性能指标及价格，所以对网络设备的需求也决定了企业网络功能的要求。下面简要概述设备选择时的几点标准。

企业所有的网络设备都需要支持可配置管理，支持一些常见的网络协议需求如 Telnet、SSH、SNMP 等。

网络设备要具有较高的拓展和转发性能，可以实现数据包在网络里进行快速传播，避免网络拥塞。

网络设备安全至关重要，企业所有的设备都需要设备自身支持基本网络安全协议来保护网络运行的安全性，企业可以考虑购买相应网络安全设备来进行安全性管理。

设备访问需求

- (1) 控制内部特定部门禁止访问外部网络，其他部门正常访问
- (2) 防止外部的 IP 地址欺骗内部主机
- (3) 总公司财务服务器，只允许财务部的员工访问。
- (4) 外网用户可以通过内网服务器端口映射实现访问公司的功能
- (5) 总公司和分公司部门之间可以互访且出口实现冗余

企业网络需求

- (1) 各交换机之间配置 Eth-trunk 实现链路冗余
- (2) 核心交换机作为用户网关实现 VLAN 间路由
- (3) 利用 DHCP 使所有用户均为自动获取 IP 地址
- (4) 出口路由配置 NAT 实现地址转换
- (5) 所有设备都可以被虚拟 telnet 远程管理

2.4 IP 规划

表 1 VLAN 划分表

类目	端口描述	IP	子网掩码	网关
总公司 网络规 划	LW2	192.168.255.2	255.255.255.0	192.168.255.1
	LW3	192.168.255.3	255.255.255.0	192.168.255.1
	LW4	192.168.255.4	255.255.255.0	192.168.255.1

类目	端口描述	IP	子网掩码	网关
	LW5	192.168.255.5	255.255.255.0	192.168.255.1
	LW6	192.168.255.6	255.255.255.0	192.168.255.1
	LW7	192.168.255.7	255.255.255.0	192.168.255.1
	LW8	192.168.255.8	255.255.255.0	192.168.255.1
	LW9	192.168.255.9	255.255.255.0	192.168.255.1
	PC1	192.168.10.X	255.255.255.0	192.168.10.1
	研发部	192.168.20.X	255.255.255.0	192.168.20.1
	市场部	192.168.30.X	255.255.255.0	192.168.30.1
	财务部	192.168.40.X	255.255.255.0	192.168.40.1
分公司网络规划	AR4	192.168.104.1	255.255.255.252	
	AR5	192.168.105.1	255.255.255.252	
	AR6	192.168.106.1	255.255.255.252	
	市场部	192.168.100.2	255.255.255.0	
	研发部	192.168.150.2	255.255.255.0	
	财务部	192.168.200.2	255.255.255.0	
内网服务器	CLIENT3	192.168.200.X	255.255.255.0	192.168.200.1
	CLIENT3-1	192.168.200.X	255.255.255.0	192.168.200.1
	LW8	192.168.255.8	255.255.255.0	
外网客户端及服务器	AR2	13.1.1.6	255.255.255.248	
	AR3	12.1.1.6	255.255.255.248	
	Server3	9.9.9.9	0.0.0.255	
	Client3	7.7.7.7	0.0.0.255	

3 网络技术选型

3.1 VLAN

VLAN 可以解决本公司网络中遇到的实际问题。使用 VLAN 可以将逻辑基础设施与物理设施分开，提供一个单一的主干网。几个不同的 VLAN 数据包可以同时通过一条中继线传输，大大节省了网络所需的中继线数量。此外，通过支持 VLAN 的网络管理软件，可以轻松地动态创建和重新配置 VLAN，使整个网络更加集中、灵活和易于管理。同时也提高了网络安全性。在交换机 LW1 上划分 vlan 10 和 vlan 20 并将接口划入 VLAN。

3.2 NAT

NAT 是指网络地址转换，装有 NAT 软件的路由器叫做 NAT 路由器，它至

少有一个有效的外部全球 IP 地址（公网 IP 地址）。这样，所有使用本地地址（私网 IP 地址）的主机在和外界通信时，都要在 AR1 路由器上将其本地地址转换成全球 IP 地址，才能和因特网连接。

3.3 ACL

ACL 在网络管理中，有必要阻止对某些站点的访问，同时控制某些站点的连接。本次网络建设 ACL 技术被用于接入层网络控制；在接入交换机 LW4 至 LW7 配置了 ACL 来限制部门之间的访问，可以有效保护公司内部隐私安全。

3.4 OSPF

OSPF 是一种动态的路由协议，为了让网络中实现路由的自动学习和通信。配置 ospf 使路由器没接收到其他的网段信息，网络的传输能传输给对应的直连路由和其他设备。路由器 AR1 和两个核心 LW1 与 LW2 交换机上配置了 OSPF 协议来保证企业内部网络的连通性。

3.5 VRRP

VRRP 是一种选择协议,它是一种在不改变组网的情况下,将物理上多台路由器虚拟成一个虚拟路由器的技术,此虚拟路由器由一个 Master 设备和多个 Backup 设备组成,被当作一个共享局域网内主机的缺省网关。

3.6 TELNET

Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用 telnet 程序，用它连接到服务器。终端使用者可以在 telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样，可以在本地就能控制服务器。要开始一个 telnet 会话，必须输入用户名和密码来登录服务器。项目使用路由模拟企业 Telnet 来实现网络安全部门对各个交换机控制台的跳转，从而提高网络设备运行的安全性。

4 设备选型

4.1 设备选型

表 2 设备选型

设备厂商	设备型号	设备名称
HUAWEI	S5735S-L24T4S-A1	三层交换机
HUAWEI	NetEngine AR720	路由器
HUAWEI	S1730S-L24TR-A1	接入交换机
HUAWEI	S1730S-L24TR	汇聚层交换机
HUAWEI	OceanStor 5110 V5	服务器

4.2 三层交换机选型

三层交换机选择 S5735S-L24T4S-A1，主要参数如表 3 所示。

表 3 三层交换机 S5735S-L24T4S-A1

S5735S-L24T4S-A1	
	
固定端口	24 个 10/100/1000BASE-T 以太网端口，
交换容量	1336Gbps/3.36Tbps
包转发率	51/126Mpps
管理和维护	支持 SVF 特性，设备即插即用;支持 eSight 网管系统、支持 WEB 网管特性
管理特性	SNMPv1/v2C/v3、CLI(Telnet/Console)、RMON(1, 2, 3, 9)、SSH、Syslog/Debug、NTP/SNTP、FTP、TFTP、Web、SFLOW

4.2 出口路由器选型

出口路由器选择 NetEngine AR720，主要参数如表 4 所示。

表 4 路由器 NetEngine AR720

NetEngine AR720	
	
接口	支持以太网接口、E1/CE1 接口、4G 接口
转发性能	9Mpps-25Mpps
IP 路由	支持静态路由、RIPng、OSPFv3、BGP4+、ISISv6、等价路由、策略路由等
高可靠性	板卡热插拔，保证业务连续稳定 提供企业业务的链路备份，提高业务接入的可靠性毫秒级的故障检测和判断机制，缩短业务中断时间
安全	内置防火墙、IPS、URL 过滤、多种 VPN 技术，为用户提供全面的安全防护能力

4.3 接入交换机选型

接入交换机选择 S1730S-L24TR-A1，主要参数如表 5 所示。

表 5 接入交换机 S1730S-L24TR-A1

S1730S-L24TR-A1	
	
固定端口	24 个 10/100/1000Base-T 以太网端口
交换容量	48Gbps
包转发率	35.71Mpps
管理与维护	支持 SVF 特性，设备即插即用

	支持 eSight 网管系统、支持 WEB 网管特性 支持智能堆叠 iStack 支持基于 Netconf/Yang 的云管理
安全特性	支持 BPDU Guard 支持 IP Source Guard 支持 CPP、NFPP 支持端口保护

4.4 服务器选型

服务器选择 OceanStor 5110 V5，主要参数如表 6 所示。

表 6 服务器 OceanStor 5110 V5

OceanStor 5110 V5	
	
前端通道端口类型	8/16/32 Gbps FC、1/10/25/40/100Gbps Ethernet.
硬盘类型	SSD、SAS、NL SAS
存储管理软件	主机多路径(UltraPath)、容灾管理(BCManager) 单设备管理软件(DeviceManager)、集中运维管理软件 (eSight)、远程维护管理软件(eService)
资源效率提升	智能 LUN 迁移(SmartMigration)、智能异构虚拟化 (martVirtualization)、智能多租户 (SmartMulti-tenant)、配额管理(SmartQuota)、 智能重删(SmartDedupe)、智能压缩 (SmartCompression)、智能精简配置(SmartThin)、智 能数据分级(SmartTier)、智能数据迅移 (SmartMotion)、智能数据销毁(SmartErase)

4.5 汇聚层交换机选型

汇聚层交换机选择 S1730S-L24TR，主要参数如表 7 所示。

表 7 汇聚层交换机 S1730S-L24TR

S1730S-L24TR	
	
散热方式	S1730S-L24TR
电源类型	外置电源适配器, 交流电源输入/内置 AC 电源, 交流电源输入
交换容量	百兆≥1.6Gbps 千兆≥8Gbps
包转发率	百兆≥1.19Mpps 千兆≥5.95Mpps
电源类型	支持百兆和千兆电

5. 设备配置

5.1 VLAN Trunk

```
接入层 LSW8:
<Huawei>system-view
//进入用户模式
[Huawei]un in en
//关闭泛洪的信息
[Huawei]sysname LSW8
[LSW8]int Eth-Trunk 1
[LSW8-Eth-Trunk1]mode lacp-static
[LSW8-Eth-Trunk1]trunkport g 0/0/1 0/0/2
[LSW8-Eth-Trunk1]port link-type trunk
[LSW8-Eth-Trunk1]port trunk allow-pass vlan 200
[LSW8-Eth-Trunk1]port trunk allow-pass vlan 900
[LSW8]vlan 200
[LSW8-vlan200]quit
[LSW8]vlan 900
```

```
[LSW8-vlan900]quit
<LSW8>save
<LSW8>sysview
[LSW8]port-group group-member Ethernet 0/0/2 Ethernet 0/0/3
[LSW8-port-group]port link-type access
[LSW8-port-group]port default vlan 200
核心层交换机 LSW1 配置:
<Huawei>system-view
[Huawei]un in en
[Huawei]sysname LSW1
[LSW1]int Eth-Trunk 1
[LSW1-Eth-Trunk1]mode lacp-static
[LSW1-Eth-Trunk1]trunkport g0/0/2
[LSW1-Eth-Trunk1]trunkport g0/0/5
[LSW1-Eth-Trunk1]port link-type trunk
[LSW1-Eth-Trunk1]port trunk allow-pass vlan 200 900
[LSW1-Eth-Trunk1]quit
[LSW1]vlan batch 10 20 30 40 200 900 800
[LSW1]int g0/0/1
[LSW1-GigabitEthernet0/0/1]port link-type trunk
[LSW1-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20 900
[LSW1-GigabitEthernet0/0/1]int g0/0/3
[LSW1-GigabitEthernet0/0/3]port link-type trunk
[LSW1-GigabitEthernet0/0/3]port trunk allow-pass vlan 30 900
[LSW1-GigabitEthernet0/0/3]int g0/0/4
[LSW1-GigabitEthernet0/0/4]port link-type trunk
[LSW1-GigabitEthernet0/0/4]port trunk allow-pass vlan 40 900
[LSW1-GigabitEthernet0/0/4]quit
[LSW1]int g0/0/24
[LSW1-GigabitEthernet0/0/24]port link-type access
[LSW1-GigabitEthernet0/0/24]port default vlan 800
[LSW1-GigabitEthernet0/0/24]quit
[LSW1]q
```

```
<LSW1>sa
```

接入层 LSW5 配置:

```
<Huawei>system-view
```

```
[Huawei]sysname LSW5
```

```
[LSW5]vlan 10
```

```
[LSW5-vlan10]quit
```

```
[LSW5]port-group group-member e0/0/2 e0/0/3
```

```
[LSW5-port-group]port link-type access
```

```
[LSW5-port-group]port default vlan 10
```

```
[LSW5-port-group]quit
```

```
[LSW5]int g0/0/1
```

```
[LSW5-GigabitEthernet0/0/1]port link-type trunk
```

```
[LSW5-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 900
```

```
[LSW5-GigabitEthernet0/0/1]quit
```

```
[LSW5]vlan 900//配置 telnet 的时候会用到
```

```
[LSW5-vlan900]quit
```

```
[LSW5-vlan900]quit
```

```
[LSW5]quit
```

```
<LSW5>save
```

接入层 LSW6:

```
<Huawei>system-view
```

```
[Huawei]sysname JR_SW6
```

```
[LSW6]vlan batch 20 900
```

```
[LSW6]int e0/0/1
```

```
[LSW6-Ethernet0/0/1]port link-type access
```

```
[LSW6-Ethernet0/0/1]port default vlan 20
```

```
[LSW6-Ethernet0/0/1]quit
```

```
[LSW6]int g0/0/1
```

```
[LSW6-GigabitEthernet0/0/1]port link-type trunk
```

```
[LSW6-GigabitEthernet0/0/1]port trunk allow-pass vlan 20 900
```

```
[LSW6-GigabitEthernet0/0/1]quit
```

```
[LSW6]quit
```

```
<LSW6>save
```

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/406205103145010120>