目录

启元公司网络规划与设计方案

1 企业简介

启元药业有限公司（以下简称启元公司）集研发、生产、销售为一体，具备原料药和各类中西药制剂生产能力，原料药红霉素系列、盐酸四环素系列、阿维菌素系列、维生素系列凭借领先的技术、优良的品质、规模化的生产以及强劲的发展势头，树誉中外。主导产品红霉素、盐酸四环素系列原料药规模占据世界首位，销售市场遍布世界各地。

公司秉承“诚信为本、效率至上”的企业理念，以“筑誉世界，康健华夏”为宗旨，始终把人民群众的用药安全、有效作为企业的使命，凭借始终如一的产品质量，使企业得到市场的广泛认同，连续多年获得区、市级“守合同，重信用"企业称号。公司被评定为国家重点高新技术企业、科技兴贸全国百家重点出口企业，建有国家级企业技术中心，国家级博士后工作站。盐酸四环素原料药通过了美国 FDA 认证、欧洲 COS 认证和欧盟的 EUGMP 认证。各剂型所有生产车间均已通过国家 GMP 认证。

在新的历史时期，启元药业以科学发展观为指导，以先进的科研、技术、管理，充分发挥宁夏区域优势，并以大市场为背景，高起点规划，鼎力打造宁夏医药面向中国、面向世界医药市场的强势产品、优势企业。自 2003 年起公司连续投资 10 多亿元完成了红霉素系列产品技改工程项目以及其它配套项目，使启元药业的发酵规模名列全国前茅，跻身于中国制药企业百强之一。在发展过程中，公司坚持清洁生产，源头治理，始终把环保工作作为“生命工程”来抓，不断采用先进的环保技术，几年来，公司共投资 2 亿多元人民币，用于环保设施的建设，环保项目走在所有项目的前面，实现了经济效益和环境效益双赢。

2 项目需求分析

启元公司多年来凭借着高质量的产品，良好的信誉优质的服务，取得用户的一致好评，积累了良好的口碑，让企业迅速的发展壮大。目前的企业的网络环境已经不能满足自身发展的需求，加上网络设备使用的年限问题，为了企业以后的长远发展，企业决定对整个网络环境进行重新部署。

要求如下：

1、将所有的老设备都进行更换，并且保证新设备有六年以上使用寿命。

2、新的网络环境需要满足企业业务及日常使用。

3、公司网络在出现问题后能够迅速的发现问题所在。

4、新的网络环境能够满足未来几年企业发展对网络的需求。

5、企业的每个部门都能够访问服务器.

6、网络环境需要一定的可靠性。

7、网络部署要与现有网络兼容。

2.1 项目设计原则

安全：在网络设计中，应充分注意系统的安全性，采用不少于两种安　全防范技术和措施，保障系统的安全，包括数据安全、设备安全、各种应用系统的安全。

高可用性：网络结构设计上要充分考虑到系统运行的可用性，要考虑各种设备配置对稳定性的影响、尽量减少单点故障，保证系统 24 小时不间断运行。

可扩展性：网络结构要易于扩展，可以在资源不足的情况向方便的进行资源的扩充，可随着使用人员的增加而能方便地进行扩展。

易维护：网络结构设计要易于维护，各种设备使用统一的网关协议 SNMP，设备命名和网络实施和有统一的规范以便于后期的维护。

2.2 公司各部门人数统计

公司包括生产部、研发部、销售部等部门，各部门人数如表 1 所示：

表 1　公司各部门及员工宿舍人数统计

部门	人数
生产部	900
研发部	245
办公部	78
销售部	200

3 网络技术选型

3.1 公司网络拓扑图规划

公司的网络主要由接入层交换机、核心层交换机、核心路由器等组成。接入层各端口根据具体需要，分别接入生产部、研发部、办公部、销售部对应的 VLAN。网络拓扑如图 1 所示：

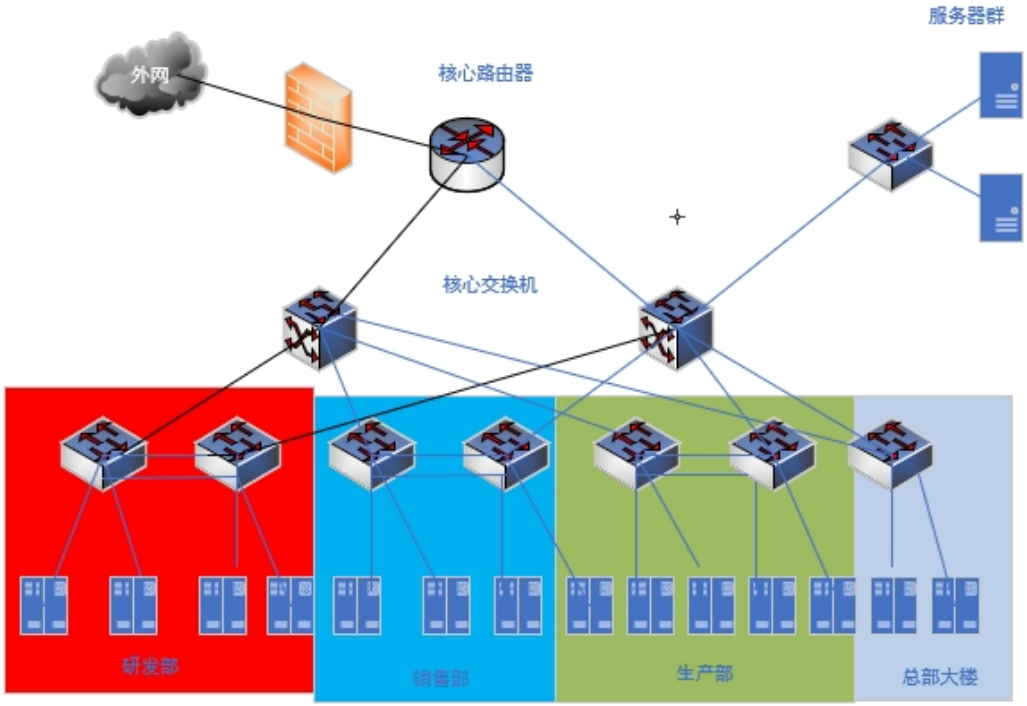

图 1 网络拓扑图

3.2 部门 VLAN 规划

设备按照部门进行 VLAN 划分和网段规划，如表 2 所示：

表 2 部门 VLAN 划分及网段规划表

部门	IP 地址范围	VLAN 端口	网关
总楼	192.168.80.0 至 192.168.80.254	Vlan 40	192.168.80.254
生产部 1	192.168.70.0 至 192.168.70.254	Vlan 30	192.168.70.254
销售部 1	192.168.60.0 至 192.168.60.254	Vlan 20	192.168.60.254
研发部 1	192.168.50.0 至 192.168.50.254	Vlan 10	192.168.50.254
生产部 2	192.168.90.0 至 192.168.90.254	Vlan 30	192.168.90.254
销售部 2	192.168.110.0 至 192.168.110.2	Vlan 20	192，168.110.254

	54		

4 网络技术选型

4.1 链路聚合技术

随着企业的不断发展，企业的网络访问量不断的增大，导致对企业网络的可靠性与速率的需求不断的增加，所以在企业网络中，网络的可靠性与速率在设计中是十分重要的一环，而增加企业网络的可靠性就需要从交换机开始。提高交换机设备的转发速率可以在两个设备间多增加几条链路或者采用高速率端口，采用多条链路会对 IP 地址造成浪费，采用高速率端口会增大网络搭建的成本，而链路聚合技术就解决了这些问题。链路聚合是逻辑上将两条或者多条链路捆绑为一条链路，这样就达到了增加设备链路的效果且不会浪费IP 地址。链路聚合也会让网络变得更加的可靠，当配置了链路聚合的两个设备间有一条或多条链路发生故障时，网络流量依然可以进行转发而不至于因为一条链路发生故障导致整个网络瘫痪。

在本项目中，在两台汇聚交换机之间进行链路聚合配置，接入层交换机之间也进行链路聚合，提升带宽，增加网络可靠性。应用在两台核心交换机直接相连的接口，用于提升该条链路带宽，因为两台核心交换机处于核心处，工作量大，所需要交换的数据多且数据包大小较大。

4.2 VLAN 技术

VLAN 是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO 模型的第二层网络。VLAN 的划分不受网络端口的实际物理位置的限制。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。此设计中因为终端设备过多，容易引发广播风暴导致设备宕机，降低交换机性能。所以此处使用 VLAN 技术对接入层进行分割广播域，降低广播风暴发生概率，同时能够达到客户需求，阻挡某些部门之间的联系。

在本项目中，将 VLAN 应用在所有二层交换机下行接口上，为的就是隔离广播域，防止太多不必要数据帧产生并在广播域内传递，降低交换机性能，导致设备宕机。

4.3 DHCP 技术

现在 IP 地址变化频繁变化以及 IP 地址不足的情况，手动配置容易出现失

误导致 IP 地址冲突且操作繁琐。DHCP 协议采用 C/S 模式架构，客户端向服务器获取 IP 地址可以降低出错率。是应用层协议，为网络设备以及主机提供 TCP/IP 服务。即插即用性，统一管理，使用效率高，更方便管理，可跨网段实现报文的交互，交互需要用到 DHCP 中继，一般为三层交换机或者路由器。DHCP 分为自动分配，手动分配和动态分配。自动分配一般用于打印机等固定网络设备，DHCP 会分配固定的 IP 地址给它，IP 地址一般会与设备 MAC 地址绑定一起。手动分配是由管理员指定某一个 IP 地址给所需网络设备，被手动分配的 IP 地址不会被拿来进行动态分配。动态分配则是由服务器进行分配 IP 地址，有租期限制，租期到期服务器便会收回 IP 地址。此设计中网络设备较多，手动配置 IP 地址明显操作繁琐，且容易出现地址冲突，相较于 DHCP 服务器去分配更加方便快捷，对于 IP 地址的利用效率也更加优越，更加易于管理。每一台联网设备都需要唯一的 IP 地址，在 DHCP 技术还没有出现时，每一台设备都需要网络管理员手动配置 IP 地址。当网络中的设备需要移动时，比如用户和计算机需要更换部门，又或者服务器，打印机等联网设备需要移动，采用手动配置静态 IP 地址就需要网络管理员重新手动配置 IP 地址，这样既麻烦又费时。DHCP 技术就解决了这一问题。当客户端需要连接网络时，发送 DHCPDISCOVER 消息，当服务器收到了来自客户端的 DHCPDISCOVER 消息，会保留一个可用的 IP 地址，即 DHCPOFFER，客户端收到 DHCPOFFER 消息，会发送一条 DHCPREQUEST 消息来告诉服务器这个 IP 地址客户端将会租用，服务器收到 DHCPREQUEST 消息后会确定这个 IP 地址没有被使用，并以单播 DHCPACK 回复。然后客户端就可以使用这个 IP 地址进行连接网络。DHCP 技术使得服务器能够动态的为网络中的其他设备提供 IP 地址，简化了移动设备 IP 地址的分配。采用 DHCP 技术还可以避免手工配置 IP 地址时遇到 IP 地址冲突的情况，确保了整个网络的一致性。

在本项目中，将 DHCP 技术主要用于两台核心交换机的下行接口上。

4.4 NAT 技术

每一台需要联网的设备都需要有一个唯一的IP地址，随着信息时代的发展，大家对网络的需求越来越大，越来越多的设备需要加入到网络中，需要连接网络的设备是爆炸式的增长的，这导致 IPV4 地址越来越匮乏。随着这一问题越来越严重，IETF 组织实施了几种解决方案，其中包括了定义私有 IPV4 地址和公有 IPV4 地址以及私有转公网技术（NAT 技术），这对于长期而言并不能从根源上解决 IPV4 地址匮乏的问题，以后能在长期解决这一问题的只有 IPV6 技术的不断更新迭代。就目前而言，每个家庭或者个人都有着很多需要接入网络的设

备，很明显，个人和家庭不可能为每一台设备去申请一个公有地址，只能通过代理商获得一个临时的公有 IPV4 地址，这时候我们想要自己或者家庭里面每一台设备都进行联网就离不开私有地址和 NAT 技术。NAT 它通过允许在内部使用私有 IPV4 地址进行通信，在需要用到公有地址的时候提供转化。对于内部的设备需要将流量发送到外部网络与外部网络进行通信时，都会通过 NAT 设备，将内部使用的私有 IPV4 地址转化为申请到的公有 IPV4 地址。

企业网采用私有 IP，Internet 采用公有 IP，私有 IP 的路由不允许通告到 Internet，企业网接入 Internet 需要向运营商申请公有 IP。IPv4 公有 IP 比较稀缺，申请也需要较高的费用，普通企业只能申请少量的 IPv4 公有 IP。所以向运营商申请一小段或 1 个公有 IP，在边界设备上做网络地址转换，将私有 IP 转换成公有 IP，然后再访问 Internet。NAT 技术把数据包中的 IP 地址转换为另一个 IP 地址，也就是可以将企业网中的私有地址在需要通过网关访问外网时转换成企业申请到的公网地址，这样能有效缓解共有 IP 地址不足的情况，使用外网 IP 对外提供服务，即 Internet 访问企业的公网 IP，然后在边界设备上，将这些公网 IP 转换到内部服务器上去。此设计中因为公司内网络设备多所以需要的 IPV4 地址较多,但是申请大量公网 IP 地址成本较大且有可能造成不必要的浪费，所以运用 NAT 技术将私有地址转换成公网地址接入以太网能够节省大量费用也能缓解 IPV4 地址不足的情况。

在本项目中，将 NAT 用于防火墙的两个接口上，因为防火墙需要识别数据并且设计于网络边界上，能够更方便对于地址的转换。

4.5 MSTP 技术

处于数据链路层的网络环境中只要部署了链路冗余就会产生链路环路的情况，而目前最好能够解决链路环路的问题是生成树，当然也可以用 Tag 或者三层隔离，生成树在二层设备加入后就会开始发送 BPDU 报文，里面携带的桥优先级和桥 ID_Mac 能够选定根桥，根桥确定后流量转发将由根桥优先处理，这就出现因配置不当导致流量从上行交换机转发到下行处理的问题，当然经验丰富的工程师实际情况中不会出现这些问题，早期的生成树因收敛速度慢，最快 30s 的原因目前已经被淘汰，取而代之的是经过改良的 RSTP 即快速生成树，虽然收敛得到改善但它还是不太适用当下的网络环境，即单域生成树，不能实现链路冗余和负载转发，因此多域生成树是目前能够快速收敛和冗余负载转发的生成树。

基于实例计算出多颗生成树，实例间实现负载分担，通过 MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个多生成树实例 MSTI，MSTP 网络中包含 1 个或多个 MST 域（MST Region），每个 MST Region 中包含一个或多个 MSTI。组成 MSTI 的是运行 STP/RSTP/MSTP 的交换设备，MSTI 是所有运行 STP/RSTP/MSTP 的交换设备经 MSTP 协议计算后形成的树状网络。此设计中在接入层交换机与核心交换机上进行 MSTP 配置，进行防环与负载均衡。

在本项目中，将 MSTP 技术应用于核心交换机与所有二层交换机直接的连接口，防止产生环路导致广播风暴，使设备宕机。

4.6 VRRP 技术

前面提到冗余技术中的网关冗余，网关冗余算是网络中比较熟悉的容错协议，它允许在“局域网”内的多个设备上使用同一个 IP 地址并且不会报错和冲突检测的协议，网关冗余能够将网关虚拟出多个从而当一台网关出现问题的时候快速切换到另一台继续工作，其中包含了优先级所以它的缺点是在网络中必须选出主网关和备网关且两台在同一个网关下同时工作，另外还需要搭配 Track 检测才能够检测上行链路进行切换，当不配置的时候是无法切换的，因此在网络部署环境中需注意，其次使用虚拟网关最好能够搭配多域生成树组网，实现在网关冗余的情况下对链路进行负载转发，充分利用好 VRRP。

VRRP 技术通过在冗余网关间共享虚拟 MAC 和 IP 地址，保证数据转发时并不是转给某一个具体网关的 IP，而是把数据转发给虚拟网关的 IP，因此，不论哪一个路由器成为主路由，都不会影响数据通信。通过组播协议对数据端口进行监控，一旦检测数据转发的端口坏掉，主路由器会停发 HELLO 包，备路由器提升为主路由，实现数据的稳定高效转发。通过在冗余网关间共享虚拟 MAC 和 IP 地址，保证数据转发时并不是转给某一个具体网关的 IP，而是把数据转发给虚拟网关的 IP，因此，不论哪一个路由器成为主路由，都不会影响数据通信。通过组播协议对数据端口进行监控，一旦检测数据转发的端口坏掉，主路由器会停发 HELLO 包，备路由器提升为主路由，实现数据的稳定高效转发。此设计中通过将 VRRP 与 MSTP 技术进行链路捆绑，来提升网络可靠性。

在本项目中，将 VRRP 技术应用在两台核心交换机的下行接口上，形成主备备份，来维持虚拟网关，提高网络的可靠性。

4.7 IRF 技术

弹性扩展：可以按照用户需求实现弹性扩展，保证用户投资。成员设备之间物理端口支持聚合功能，IRF 系统和上、下层设备之间的物理连接也支持聚合功能，这样通过多链路备份提高了链路的可靠性；IRF 系统由多台成员设备组成，一旦 Master 设备故障，系统会迅速自动选举新的 Master，以保证通过系统的业务不中断，从而实现了设备级的 1：N 备份；IRF 系统会有实时的协议热备份功能负责将协议的配置信息备份到其他所有成员设备，从而实现 1：N 的协议可靠性。简化管理：IRF 架构形成之后，可以连接到任何一台设备的任何一个端口就以登录统一的逻辑设备，通过对单台设备的配置达到管理整个智能弹性系统以及系统内所有成员设备的效果，而不用物理连接到每台成员设备上分别对它们进行配置和管理。因此，IRF 技术能够轻易的将设备的交换能力、用户端口的密度扩大数倍，从而大幅度提高了设备的性能。

在本项目中，在接入层交换机实行软堆叠来提高设备性能，也方便后续管理员对于接入层网络设备的管理，主要是运用在研发部两台交换机之间的连接接口，销售部两台交换机之间的连接口以及生产部两台交换机之间的连接口。

4.8 OSPF 技术

OSPF 适合在大范围的网络：OSPF 协议当中对于路由的跳数，它是没有限制的，所以 OSPF 协议能用在许多场合，同时也支持更加广泛的网络规模。只要是在组播的网络中，OSPF 协议能够支持数十台路由器一起运作。OSPF 协议的设计是为了避免路由环路：在使用最短路径的算法下，收到路由中的链路状态，然后生成路径，这样不会产生环路。此设计中在核心层路由器与两个核心交换机上进行 OSPF 配置，相比于静态配置，使用 OSPF 要更加简便快捷。OSPF（开放最优路径优先）是一种动态路由协议，相比于 RIP 有着巨大优势，RIP 存在着收敛慢，不能到达远端路由以及不能选择最优路径进行转发等缺点，而 OSPF 技术正好解决了 RIP 技术的这些缺点。OSPF 有着收敛快，不限定跳数，将链路宽带作为选择路径的参考值的特点。目前中小型的网络环境中 OSPF 已经成为主流的动态路由配置协议。

在本项目中，将 OSPF 技术运用在核心交换机与路由器上的所有接口，确保它们的路由表非常齐全，不会出现链路不同的情况，提升网络可靠性。

5 网络设备选型

5.1 核心交换机

核心交换机如图 2 所示：

图 2 核心交换机 RG-S5760C-24SFP/8GT8XS-X

交换机参数

转发性能：426Mpps/600Mpps

接口数量：24 个 SFP 光口（含 8 个 COMBO 口），8 个 10G 光口用于上联

整机交换容量：1.36 Tbps/13.6 Tbps

管理口：1 个 MGMT 端口、1 个 Console 端口、1 个 USB 端口，符合 USB2.0 的标准

扩展槽：预留 2 个扩展插槽（RG-S5760C-48GT4XS-HP-X 、RG-S5760C-48SFP4XS-X 预留 1 个拓展 插槽），可用于扩展业务板卡和管理板卡

5.2 接入层交换机

接入层交换机如图 3 所示：

图 3 接入交换机 RG-S5310-48GT4XS-E

交换机参数

固定端口：48 个 10/100/1000M 自适应电口，4 个 1G/10G SFP+光口

交换容量：672Gbps/6.72Tbps

包转发率：196Mpps/252Mpps

支持二层链路聚合 支持 STP、RSTP、MSTP，MSTP 实例数量 65 个，出现链路故障后，各个设备能够进行生成树的重新计算。

5.3 核心路由器

核心路由器如图 4 所示：

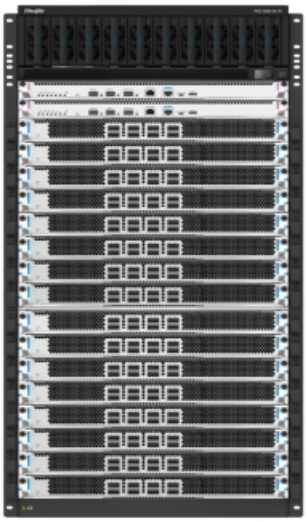

图 4 核心路由器 RG-N8018-R

路由器参数

交换容量：409.6Tbps

转发性能：92753Mpps

主控数量：2

网板槽位：4

线卡插槽：16

业务板插槽：最大 64

5.4 防火墙

防火墙如图 5 所示。

图 5 防火墙 RG-WALL 1600-Z3200

防火墙参数

固化千兆电口 8 个 GE 电口

固化千兆光口 1 个 GE 光口

固化万兆光口 1 个 10GE 光口

管理口 1 个数据复用口（Ge 0/0)

Console 接口 1 个

USB 接口 2 个 USB 2.0 接口

硬盘 标配无，可扩展 1TB 硬盘

电源 单电源

6 网络设备配置

6.1 核心路由器

```
en  #进入系统视图
conf t  #进入特权模式
hostname R1  #修改设备名
int g0/1  #进入指定接口
ip add 192.168.10.1 255.255.255.0  #配置 IP 地址及子网掩码
no shut  #激活接口
int g0/2  #进入指定接口
ip add 192.168.20.1 255.255.255.0  #配置 IP 地址及子网掩码
no shut  #激活接口
int look 0  #创建 lookpback 0
ip add 1.1.1.1 255.255.255.255  #配置 IP 地址及子网掩码
ex  #返回上一模式
ip ospf 1  #配置 ospf
router-id 1.1.1.1  #创建路由 id
net 1.1.1.1 0.0.0.0 area 0  #发布 lookpback 0
net 192.168.200.0 0.0.0.255 area 0  #发布上连网段
net 192.168.10.0 0.0.0.255 area 0  #发布下连网段
net 192.168.20.0 0.0.0.255 area 0  #发布下连网段
ex  #返回上一模式
int s0/0  #进入指定接口
ip add 192.168.200.1 255.255.255.0  #配置 IP 地址及子网掩码
no shut  #激活接口
```

6.2 核心交换机 1

```
En  #进入系统视图
conf t  #进入特权模式
hostname HJ1  #修改设备名
```

```
ip routing  #开启路由功能
vlan 10   #创建 vlan
vlan 20  #创建 vlan
vlan 30  #创建 vlan
vlan 40  #创建 vlan
ex  #返回上一模式
int g0/1  #进入指定接口
no sw  #不是交换机接口
ip add 192.168.10.2 255.255.255.0  #配置 IP 地址及子网掩码
no shut  #激活接口
exit  #返回上一模式
int aggregatePort 1  #创建聚合接口
switchport mode trunk   #修改接口模式为 trunk
switchport trunk all  #放通所有 vlan
exi  #返回上一模式
int r gi0/6 - 7  #进行批量接口配置
port-group 1 mode active  #接口组模式改为动态模式
int g0/2  #进入指定接口
sw mo tr  #修改接口模式为 trunk
sw tr vl all  #放通所有 vlan
Int g0/3  #进入指定接口
sw mo tr  #修改接口模式为 trunk
sw tr vl all  #放通所有 vlan
int g0/4  #进入指定接口
sw mo tr  #修改接口模式为 trunk
sw tr vl all  #放通所有 vlan
int g0/5  #进入指定接口
sw mo tr  #修改接口模式为 trunk
sw tr vl all  #放通所有 vlan
ex  #返回上一模式
span mst con  #域生成树模式
rev 1  #校订 1
name aaa  #域命名
```