|  |  |
| --- | --- |
| 学院标志(改) 副本 | 惠州学院  HUIZHOU UNIVERSITY |

网络工程课程设计报告

**题目：** **XXX企业的网络规划方案**

**姓 名 何树深**

**学 号 1314080903212**

**专业班级 13网络2班**

**指导教师 蔡招权**

**提交日期 2015-12-15**

教务处制

XXX企业的网络规划

[第一章：需求分析 4](#_Toc22795)

[1.1 企业背景 4](#_Toc2552)

[1.2 企业物理结构 4](#_Toc17968)

[1.3 需求 4](#_Toc32062)

[第二章：网络规划 5](#_Toc19173)

[2.1 分层模型 5](#_Toc10153)

[2.1.1 核心层 5](#_Toc9630)

[2.1.2 汇聚层 5](#_Toc32432)

[2.1.3 接入层 5](#_Toc2972)

[2.2 分层模型的优点 7](#_Toc10658)

[2.3 网络拓扑图 7](#_Toc6559)

[2.4 信息点分布 8](#_Toc25133)

[第三章： 设备选型 8](#_Toc6882)

[3.1 设备选型原则 8](#_Toc26075)

[3.2 设备清单 9](#_Toc24854)

[第四章：数据中心 10](#_Toc26783)

[4.1 数据中心机房的设计与温湿度环境要求 10](#_Toc32073)

[4.2 数据中心的结构 10](#_Toc14508)

[4.2.1数据中心的含义 10](#_Toc26831)

[4.2.2 数据中心层次划分 11](#_Toc1582)

[4.2.3 数据中心的结构图 11](#_Toc26282)

[4.3 存储阵列 12](#_Toc5531)

[4.3.1 存储阵列系统的硬件组成 12](#_Toc26888)

[4.3.2 各种级别的磁盘阵列的应用 12](#_Toc6580)

[4.4 存储网络 12](#_Toc25544)

[4.4.1 存储网络常见类型 12](#_Toc6771)

[4.4.2 存储区域网络型(SAN)介绍 12](#_Toc31792)

[4.4.3 存储区域网络型(SAN)的常用示意图 13](#_Toc14449)

[4.4.4 企业中的应用 13](#_Toc18225)

[第五章：子网划分方案 14](#_Toc22678)

[5.1 信息楼 14](#_Toc4846)

[5.2 研发楼 14](#_Toc25089)

[5.3 营销楼 14](#_Toc23909)

[5.4 财务楼 15](#_Toc18579)

[5.5 生产楼 15](#_Toc26981)

[5.6 VLAN划分 15](#_Toc12426)

[5.6.1 VLAN划分的好处 15](#_Toc11322)

[5.6.2 VLAN的划分方法 15](#_Toc7163)

[5.6.3 VLAN划分方案 16](#_Toc25015)

[第六章：网络管理 16](#_Toc22842)

[6.1 网络管理的定义 16](#_Toc16767)

[6.2 网络管理的主要功能 16](#_Toc24945)

[6.3 网络管理系统 17](#_Toc26567)

[6.3.1 网络管理系统的主要功能 17](#_Toc4337)

[6.3.2 网络故障管理示意图 17](#_Toc21728)

[第七章：安全防护 18](#_Toc12033)

[7.1 网络安全的定义 18](#_Toc16964)

[7.2 保护网络安全的主要措施 18](#_Toc10554)

第一章：需求分析

## 1.1 企业背景

XXX为一家员工2000的企业。

该企业的主要建筑有:研发楼、营销楼、财务楼、信息楼、生产楼。每栋楼7层， 各建筑间距离均在2km内。

## 1.2 企业物理结构

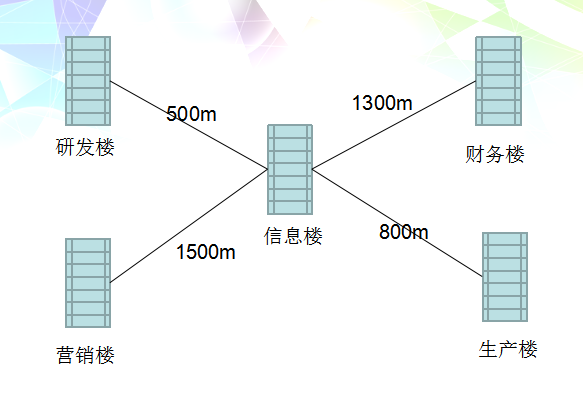
信息楼： 位于中心位置，主要存放各类设备， 各类设备的管理部门也在其中。

研发楼： 距离信息楼500m， 主要是研发类的部门。

财务楼： 距离信息楼1300m， 主要是财务类部门。

营销楼： 距离信息楼1500m， 销售类部门和售后服务等部门。

生产楼： 距离信息楼800m。



## 1.3 需求

1. . 千兆干线，百兆到桌面。
2. . 能实现统一的网络管理、维护。
3. . 网络的适应性和可拓展性要强， 方便日后升级、更改。
4. . 要确保整个计算机网络系统的可靠性、安全性，具有一定的冗余。容错能力强，确保信息处理安全保密。
5. . 管理系统的使用要求简单易学， 方便非计算机专业人员的使用。
6. . 搭建各类需要的服务器。
7. . 要求采用适合的存储方式， 保证企业数据的安全、稳定和快速访问。
8. . 网络本身的安全也要得到保障。

# 第二章：网络规划

## 2.1 分层模型

### 2.1.1 核心层

核心层层是局域网的主干，其主要目的是尽可能快地交换数据。网络的这个分层不应该被牵扯到费力的数据包操作或者任何减慢数据交换的处理。应该避免在核心层使用如访问控制列表和数据包过滤这类的功能。

核心层主要负责以下的工作：

1). 提供交换区块间的连接；

2). 提供到其他区块(如服务器区块)的访问；

3). 尽可能快地交换数据帧或数据包。

### 2.1.2 汇聚层

网络的汇聚层是网络接入层和核心层之间的分界点。汇聚层也帮助定义和区分网络核心层。该分层提供了边界定义，并在该处对潜在费力的数据包操作进行处理。

在局域网环境中，汇聚层执行最多的功能有：

1). VLAN的聚合；

2). 部门级或工作组接入；

3). 广播域咸多点广播域定义；

4). VLAN间路由；

5). 介质转换及安全等。

### 2.1.3 接入层

网络的接入层是最终用户被许可接入网络的点。该层能通过滤或访问控制列表提供对用户流量的进一步控制；不过，该分层的主要功能是为最终用户提供网络接入。

在局域网环境中，接入层主要功能如下：

1). 到汇聚层的工作组连接

2). 建立单独的冲突域(分段)

3). 共享式带宽或交换式带宽

4). 提供灵活的用户接入及扩展

## 2.2 分层模型的优点

1). 冗余： 适当的冗余能防止单点故障， 提高性能；

2). 可伸缩性：分层网络伸缩性非常好，模块化设计允许你在网络扩大时直接复制设计元素，因为模块的每一个实例都是一致的，网络扩展更易于规划和实施。

3). 性能： 使用了冗余， 实现负载均衡，避免竞争，可以有效提高性能。

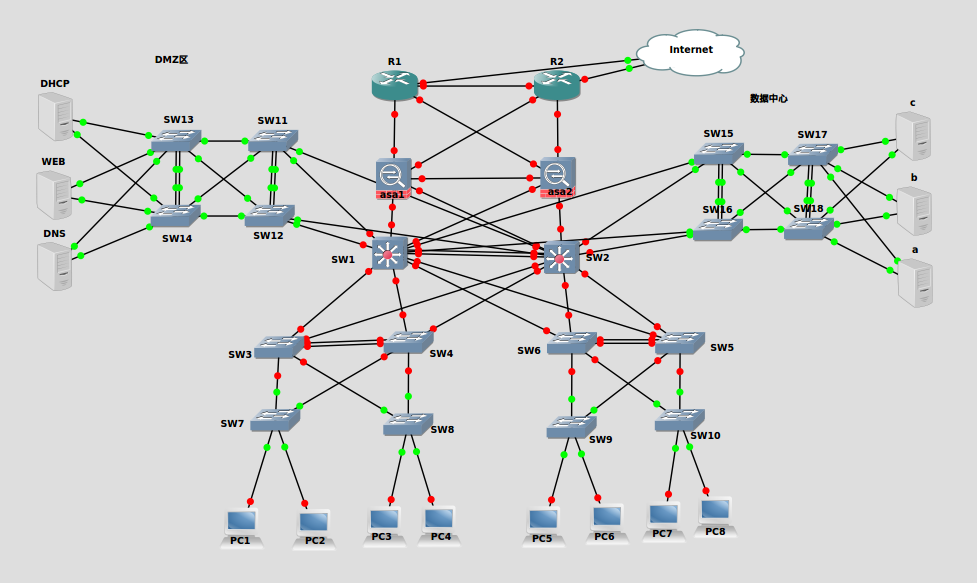
4). 可管理性和可维护性：因为分层网络天生就是模块化的，且具有很好的伸缩性，因此可维护性和可管理性自然也就很好，对于其它网络拓扑设计，可管理性会随网络的增长变得越来越复杂。

5). 安全性：可在不同的层次上提供不同的安全策略， 提高安全性。

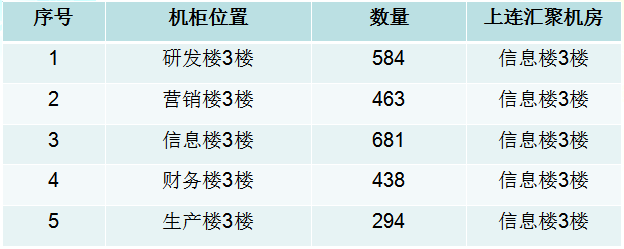
## 2.3 网络拓扑图

左翼是DMZ区域，采用冗余+分层。右翼是“数据中心”，同样采用冗余+分层。

从下往上第一层是用户层， 第二层是接入层， 第三层是汇聚层， 第四层是核心层， 第五层是防火墙， 第六层是路由器。



## 2.4 信息点分布



# 第三章： 设备选型

## 3.1 设备选型原则

1). 厂商的选择

所有[网络设备](http://baike.baidu.com/view/1158081.htm" \t "http://baike.baidu.com/_blank)尽可能选取同一厂家的产品，这样在设备可互连性、协议互操作性、技术支持和价格等方面都更有优势。从这个角度来看，产品线齐全、技术认证队伍力量雄厚、产品市场占有率高的厂商是网络设备品牌的首选。其产品经过更多用户的检验，产品成熟度高，而且这些厂商出货频繁，生产量大，质保体系完备。作为[系统集成商](http://baike.baidu.com/view/907450.htm" \t "http://baike.baidu.com/_blank)，不应依赖于任何一家的产品，应能够根据需求和费用公正地评价各种产品，选择最优的。在制定网络方案之前，应根据用户承受能力来确定网络设备的品牌。

2). 扩展性

在网络的[层次结构](http://baike.baidu.com/view/420833.htm" \t "http://baike.baidu.com/_blank)中，主干设备选择应预留一定的能力，以便将来扩展，而低端设备则够用即可，因为低端设备更新较快，且易于扩展。由于企业网络结构复杂，需要[交换机](http://baike.baidu.com/view/1077.htm" \t "http://baike.baidu.com/_blank)能够接续全系列接口，例如光口和电口、百兆、千兆和万[兆](http://baike.baidu.com/view/149761.htm" \t "http://baike.baidu.com/_blank)端口，以及多模光纤接口和长距离的单模光纤接口等。其交换结构也应能根据网络的扩容灵活地扩大容量。其软件应具有独立知识产权，应保证其后续研发和升级，以保证对未来新业务的支持。

3). 可靠性

由于升级的往往是核心和骨干网络，其重要性不言而喻，一旦瘫痪则影响巨大。

4). 可管理性

一个大型网络可管理程度的高低直接影响着运行成本和业务质量。因此，所有的节点都应是可网管的，而且需要有一个强有力且简洁的[网络管理系统](http://baike.baidu.com/view/2523209.htm" \t "http://baike.baidu.com/_blank)，能够对网络的业务流量、运行状况等进行全方位的监控和管理。

5). 安全性

随着网络的普及和发展，各种各样的攻击也在威胁着网络的安全。不仅仅是接入[交换机](http://baike.baidu.com/view/1077.htm" \t "http://baike.baidu.com/_blank)，骨干层次的交换机也应考虑到安全防范的问题，例如[访问控制](http://baike.baidu.com/view/469056.htm" \t "http://baike.baidu.com/_blank)、[带宽](http://baike.baidu.com/view/10821.htm" \t "http://baike.baidu.com/_blank)控制等，从而有效控制不良业务对整个骨干网络的侵害。

6). QoS控制能力

随着网络上多媒体业务流（如语音、视频等）越来越多，人们对核心交换节点提出了更高的要求，不仅要能进行一般的[线速交换](http://baike.baidu.com/view/5920124.htm" \t "http://baike.baidu.com/_blank)，还要能根据不同的业务流的特点，对它们的优先级和[带宽](http://baike.baidu.com/view/10821.htm" \t "http://baike.baidu.com/_blank)进行有效的控制，从而保证重要业务和时间敏感业务的顺畅。

7). 标准性和开放性

由于网络往往是一个具有多种厂商设备的环境，因此，所选择的设备必须能够支持业界通用的开放标准和协议，以便能够和其他厂商的设备有效地互通。

## 3.2 设备清单

1). 核心交换机2台。

2). 路由器2台。

3). 汇聚层交换机，每栋楼2台，DMZ区域2台， 数据中心2台。

4). 接入层交换机，2400/24=100台，DMZ区域2台， 数据中心2台。

5). 防火墙2台。

6). 流控设备2台，独立于防火墙，提供更好的流量控制。

7). 磁盘阵列设备1台， 用于数据中心的数据存储。

8). 服务器4台：DHCP服务器， DNS服务器， WEB服务器， FTP服务器

|  |  |  |
| --- | --- | --- |
| 序号 | 设备 | 数量(台) |
| 1 | 核心层交换机 | 2 |
| 2 | 路由器 | 2 |
| 3 | 汇聚层交换机 | 14 |
| 4 | 接入层交换机 | 104 |
| 5 | 防火墙 | 2 |
| 6 | 流控设备 | 2 |
| 7 | 磁盘阵列设备 | 1 |
| 8 | 服务器 | 4 |

# 第四章：数据中心

广义的数据中心是企业（机构）的业务系统与数据资源进行集中、集成、共享、分析的场地、工具、流程的有机组合。其核心内容包括业务系统、数据ETL、ODS数据库、数据仓库、数据集市、商务智能等，也包括物理的运行环境（中心机房）和运行维护管理服务。

## 4.1 数据中心机房的设计与温湿度环境要求

1). 污染物。远离腐蚀气体、易燃易爆物；腐蚀气体随着新风吸入机房后会对计算机设备和人员健康造成危害，同时不洁净的空气也会对计算机设备的运行造成不利影晌，还会对机房内精密空调、新风机等的滤网等造成污染。[4]

2). 温度、湿度。  
　　 温度和湿度必须被严格控制，以提供可连续运行的温度和湿度范围。  
　　 干球温度计:20℃~25℃(68F~77F)。  
　　 相对湿度:40%~50%。  
　　 最大露点:15℃(59℉)。

最小露点：5.5℃(41.9℉)。

最大变化速度:每小时5℃(9℉)。

3). 噪声。计算机系统停机时，机房内的噪声在主机房中心处测试应小于65dB(A)。  
　　4). 照度。计算机机房在距地0.8m处，照度不应低于300lx，辅助房间照度不低于200lx。  
　　5). 无线电干扰场强。在频率为0.15~1000MHz时不大于126dB。  
　　6). 磁场干扰场强不大于800A/m。  
　　7). 在计算机系统停机条件下，主机房地板表面垂直及水平向的振动加速度值不应大于5OOmm/s。  
　　8). 主机房地面及工作台面的静电泄漏电阻，应符合现行国家标准GE6650一1986《计算机机房用活动地板技术条件》的规定。

## 4.2 数据中心的结构

### 4.2.1数据中心的含义

1). 数据中心提供所有的应用系统（包括集中的业务应用系统、数据交换平台、应用集成平台）的运营环境；

2). 数据中心是容纳用以支持应用系统运行的基础设施（包括机房、服务器、网络、存储设备）的物理场所；

3). 数据中心包括数据中心本身的ODS、数据仓库及建立在其上的决策分析应用；

4). 数据中心有一套成熟的运行、维护体系支持其日常运行，保证应用系统高效、准确、不间断地运行。

### 4.2.2 数据中心层次划分

1). 基础设施层：用统一的技术将机房、通信、计算、存储等IT基础资源融合形成数据中心的基础设施，为业务系统提供基本的资源服务，提高资源利用率以及IT系统的可靠性。

2). 基础软件层：信息资源是企业生产过程中所涉及的一切文件、资料、图表和数据等信息的总称。本层存储了企业 （机构）生产和经营活动所产生、获取、处理、存储、传输和使用的一切信息资源。

3). 管理调度：实现存储资源化、计算资源化、网络资源化，并能够动态调整资源匹配数据的读写存储，解决统一管理难的问题；

4). 应用层：主要包括针对结构化和非结构化数据的各种应用。包括种业务系统、辅助决策系统和各种多媒体应用（监控、流媒体、统一通信 、呼叫中心、视频会议 、VOIP）。

### 4.2.3 数据中心的结构图



## 4.3 存储阵列

### 4.3.1 存储阵列系统的硬件组成

1). 控制框

控制框用于处理各种存储业务，并管理级联在控制框下面的硬盘框。

2). 硬盘框

硬盘框主要用于容纳各种硬盘，为应用服务器提供充足的存储空间。

### 4.3.2 各种级别的磁盘阵列的应用



## 4.4 存储网络

### 4.4.1 存储网络常见类型

DAS：直接连接存储

NAS：网络连接存储

SAN：存储区域网络

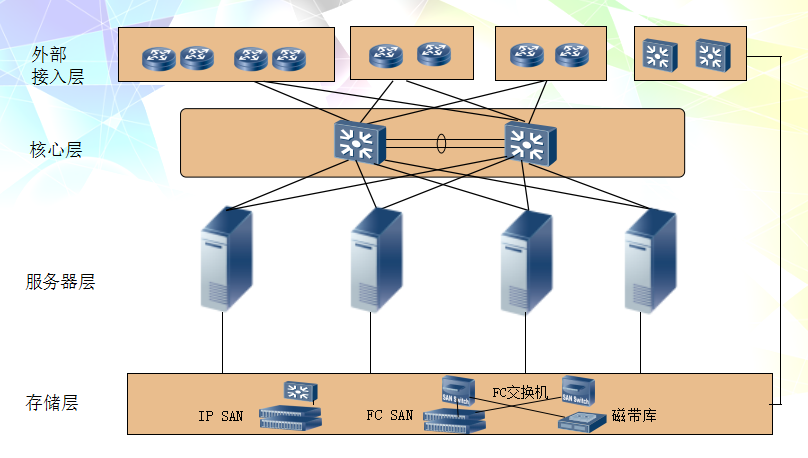
### 4.4.2 存储区域网络型(SAN)介绍

存储区域网络(Storage Area Networks，SAN)：一个存储网络是一个用在服务器和存储资源之间的、专用的、高性能的网络体系。 SAN是独立于LAN的服务器后端存储专用网络。 SAN采用可扩展的网络拓扑结构连接服务器和存储设备，每个存储设备不隶属于任何一台服务器，所有的存储设备都可以在全部的网络服务器之间作为对等资源共享。

SAN主要利用Fibre Channel protocol（光纤通道协议），通过FC交换机建立起与服务器和存储设备之间的直接连接，因此我们通常也称这种利用FC连接建立起来的SAN为FC-SAN。FC特别适合这项应用，原因在于一方面它可以传输大块数据，另一方面它能够实现较远距离传输。SAN主要应用在对于性能、冗余度和数据的可获得性都有很高的要求高端、企业级存储应用上。

随着存储技术的发展，目前基于TCP/IP协议的IP-SAN也得到很广泛的应用。IP-SAN具备很好的扩展性、灵活的互通性，并能够突破传输距离的限制，具有明显的成本优势和管理维护容易等特点。

### 4.4.3 存储区域网络型(SAN)的常用示意图



### 4.4.4 企业中的应用

1). 在企业中采用的是双交换模式的FC-SAN

2). 存储阵列采用RAID5

# 第五章：子网划分方案

## 5.1 信息楼

|  |  |  |
| --- | --- | --- |
| 序号 | 楼层 | 子网 |
| 1 | 1 | 172.17.1.0/24 |
| 2 | 2 | 172.17.2.0/24 |
| 3 | 3 | 172.17.3.0/24 |
| 4 | 4 | 172.17.4.0/24 |
| 5 | 5 | 172.17.5.0/24 |
| 6 | 6 | 172.17.6.0/24 |
| 7 | 7 | 172.17.7.0/24 |

## 5.2 研发楼

|  |  |  |
| --- | --- | --- |
| 序号 | 楼层 | 子网 |
| 1 | 1 | 172.17.11.0/24 |
| 2 | 2 | 172.17.12.0/24 |
| 3 | 3 | 172.17.13.0/24 |
| 4 | 4 | 172.17.14.0/24 |
| 5 | 5 | 172.17.15.0/24 |
| 6 | 6 | 172.17.16.0/24 |
| 7 | 7 | 172.17.17.0/24 |

## 5.3 营销楼

|  |  |  |
| --- | --- | --- |
| 序号 | 楼层 | 子网 |
| 1 | 1 | 172.17.21.0/24 |
| 2 | 2 | 172.17.22.0/24 |
| 3 | 3 | 172.17.23.0/24 |
| 4 | 4 | 172.17.24.0/24 |
| 5 | 5 | 172.17.25.0/24 |
| 6 | 6 | 172.17.26.0/24 |
| 7 | 7 | 172.17.27.0/24 |

## 5.4 财务楼

|  |  |  |
| --- | --- | --- |
| 序号 | 楼层 | 子网 |
| 1 | 1 | 172.17.31.0/24 |
| 2 | 2 | 172.17.32.0/24 |
| 3 | 3 | 172.17.33.0/24 |
| 4 | 4 | 172.17.34.0/24 |
| 5 | 5 | 172.17.35.0/24 |
| 6 | 6 | 172.17.36.0/24 |
| 7 | 7 | 172.17.37.0/24 |

## 5.5 生产楼

|  |  |  |
| --- | --- | --- |
| 序号 | 楼层 | 子网 |
| 1 | 1 | 172.17.41.0/24 |
| 2 | 2 | 172.17.42.0/24 |
| 3 | 3 | 172.17.43.0/24 |
| 4 | 4 | 172.17.44.0/24 |
| 5 | 5 | 172.17.45.0/24 |
| 6 | 6 | 172.17.46.0/24 |
| 7 | 7 | 172.17.47.0/24 |

## 5.6 VLAN划分

### 5.6.1 VLAN划分的好处

1). 有效的带宽利用—通过将网络分成小的广播域或子网，VLAN解决了在大型“平”网络中发现的扩展性问题，将所有的数据流，包括广播或多点广播，都别限制在子网中。

2). 安全性—通过在VLAN间强迫进行第三层路由选择，VLAN提供了安全性。如果配置了VLAN间通讯，可以使用路由器传统的安全和 功能。

3). 负载均衡多条通信—VLAN允许第三层路由选择协议智能决定到达目的地的最佳路径，当有多条到达目的地的路径时，还能够进行负载均衡。

4). 对故障组建的隔离—减少网络故障的影响。

### 5.6.2 VLAN的划分方法

1). 基于端口的VLAN划分

2). 基于MAC地址的VLAN划分

3). 基于网络层协议的VLAN划分

4). 基于策略的VLAN划分

5). 基于IP组播的VLAN划分

6). 基于按用户定义、非用户授权的划分VLAN

### 5.6.3 VLAN划分方案

每栋楼每层为一个VLAN， 如果每层有多个部门， 也可以按部门划分， 这样一层就会有多个VLAN。

# 第六章：网络管理

该企业的网络管理使用网络管理系统。

## 6.1 网络管理的定义

网络管理：是保障网络可靠运行的最重要手段。

网络管理员可以通过网络管理系统对网络进行全面监控。

网络管理包括对[硬件](http://baike.baidu.com/view/25278.htm" \t "http://baike.baidu.com/_blank)、软件和人力的使用、综合与协调，以便对[网络资源](http://baike.baidu.com/view/21050.htm" \t "http://baike.baidu.com/_blank)进行监视、测试、配置、分析、评价和控制，这样就能以合理的价格满足网络的一些[需求](http://baike.baidu.com/view/195818.htm" \t "http://baike.baidu.com/_blank)，如实时运行性能、[服务质量](http://baike.baidu.com/view/522662.htm" \t "http://baike.baidu.com/_blank)等。另外，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行等。网络管理常简称为网管。

## 6.2 网络管理的主要功能

1). 故障管理, 包括：

A. [故障](http://baike.baidu.com/view/553202.htm" \t "http://baike.baidu.com/_blank)报警

B. 故障[信息管理](http://baike.baidu.com/view/23634.htm" \t "http://baike.baidu.com/_blank)

C. 排错支持工具

D. 检索/分析故障信息

2). 计费管理，包括：

A. 计费[数据采集](http://baike.baidu.com/view/709701.htm" \t "http://baike.baidu.com/_blank)

B. 数据管理与数据维护

C. 计费政策制定

D. 政策比较与决策支持

E. 数据分析与费用计算

F. 数据查询

3). 配置管理，包括：

A. 配置信息的自动获取

B. 自动配置、自动备份及相关技术

C. 配置一致性检查

D. 用户操作记录功能

4). 性能管理，包括：

A. 性能监控

B. 阀值控制

C. 性能分析

D. 可视化的性能报告

E. 实时性能监控

F. 网络对象性能查询

5). 安全管理

6). 上网行为管理

## 6.3 网络管理系统

### 6.3.1 网络管理系统的主要功能

1). 显示网络拓扑图

2). 端口状态监视与分析

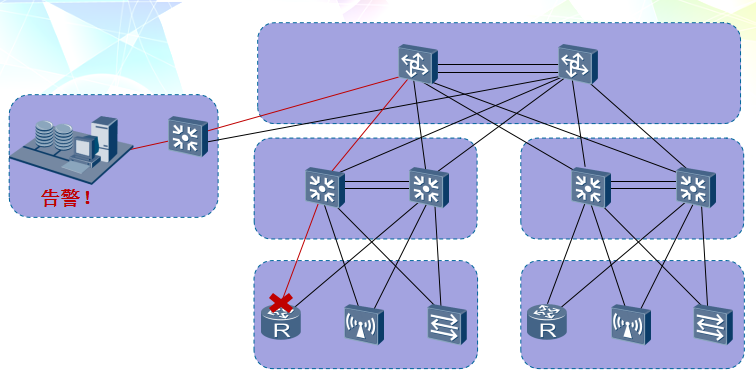
3). 网络性能与状态的图表分析

4). 故障诊断和报警

5). 简化网络设备管理

6). 具有配置VLAN的[能力](http://baike.baidu.com/view/41286.htm" \t "http://baike.baidu.com/_blank)

### 6.3.2 网络故障管理示意图



# 第七章：安全防护

该企业网络的安全主要依靠防火墙。

## 7.1 网络安全的定义

网络安全是指网络系统的[硬件](http://baike.baidu.com/view/25278.htm" \t "http://baike.baidu.com/_blank)、[软件](http://baike.baidu.com/subview/37/6030295.htm" \t "http://baike.baidu.com/_blank)及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，[网络服务](http://baike.baidu.com/view/1279152.htm" \t "http://baike.baidu.com/_blank)不中断。

## 7.2 保护网络安全的主要措施

1). 全面规划网络平台的安全策略。

2). 制定网络安全的管理措施。

3). 使用[防火墙](http://baike.baidu.com/view/3067.htm" \t "http://baike.baidu.com/_blank)。

4). 尽可能记录网络上的一切活动。

5). 注意对网络设备的物理保护。

6). 检验网络平台系统的脆弱性。

7). 建立可靠的识别和鉴别机制。