# 澳洋医院办公楼及综合楼
# 网络方案

目录

# 第一章. 概述

## 1.1 建筑群网络建设背景

目前，人类社会正处在一种伟大的转折时期，社会信息化的程度已被看作是一种国家现代化水平和综合国力的重要标志。在这个信息时代，各个单位各个部门的信息技术建设是极其重要的。因此在信息社会的今天，网络信息系统的建设尤其重要。

网络系统建成后，将为办公大楼提供高效率的办公环境，实现无纸化协同办公。网络系统的设计必须兼顾先进性、高可靠性、容错性、灵活性与安全性，提供一套可监控、易管理、可扩展、易升级的高效网络系统。实现主干千兆，并且千兆互换到桌面的高效网络系统。

本次组网是按照下面几点大的目的来考虑的，在一种健全成熟的网络体系中，这几种点是必备的。因此本次组网力争做到下面几种方面：

1. 建成较完善的局域网管理信息网络体系。实现局域网内部的可靠连接，实现网络内部各部门、各人员信息的交流与资源的共享。

2. 建立高效的网络管理中心，整个企业网络的关键设备,如中心互换机、服务器、路由器等都集中安装在网络中心.企业网络建成后，运用高效的网管软件、安全方略，可对整个企业网络实行管理和监控。

3. 建立高可靠性的网络系统，保证网络运行不间断。

4. 建立高效协同的办公环境，保证各部分的的工作人员可以有良好的交流环境，使其互相之间的协作愈加紧密，更利于发挥自己的潜能，为企业发明更多的价值。

5. 进行方略控制，严格控制内网顾客的操作权限，给不一样的人员分派不一样的权限。

6. 根据不一样的部门划分不一样的 VLAN，保证各个部门之间的

独立性，控制各个 VALN 之间的访问。

通过这样的设计后，建设后的网络是一种高效的、功能完善的、安全的、可管理的网络。对网络的性能也做了优化，选用良好的设备，保证系统的高可用性。

## 1.2 建网需求分析

### 一般建网需求

办公网网络在实际的建设过程当中，应当充足考虑到本次组网的多业务以及本企业的特点等应用需求，如：员工对服务器的访问，公网顾客对服务器的访问，波及到基础网络设施的建设和业务应用平台建设两个不一样的层面。此处重要分析办公网络基础设施建设和网络运行方面有关的内容，重要有如下几方面的特点：

1、 对 Internet 的访问需求：

将根据办公大楼实际需要，选择出口网络的带宽，通过 ISP 接入 Internt。从而可以满足企业员工的上网需求，可以满足外网访问企业 WEB、FTP、MAIL 等服务器，利于企业做好对外宣传和服务。

2、 顾客管理的需求：。

对顾客带宽进行控制的需求，规定设备能对顾客的带宽进行控制，辟如限制为 64K 、256K、512K、1M、2M、5M、10M 等等级。

3、 网络管理的需求：

整个网络的关键设备,如中心互换机、服务器、路由器等都集中安装在网络中心.企业网络建成后，运用高效的网管软件、安全方略，可对整个企业网络实行管理和监控。

4、 安全管理的需求：

1） 在目前的网络环境下，怎样保障办公网络的安全成为各个企业在组建网时不得不考虑的问题，目前重要袭击手段有 DOS、DDOS、IP 欺骗、未授权访问等。

2） 运用高性能的网络安全防御设备，在网络的出口处屏蔽掉病毒及黑客的袭击，保护内网数据的安全。

5、 组播业务的需求

伴随多种业务的融合，尤其是可控组播的需求将伴随企业信息化的深入而体现出来。

## 网络安全需求分析和对策

伴随以网络为关键的信息技术目新月异的发展，尤其是 Internet/Intranet 在全球的迅速普及，网络安全问题正日益成为人们关注的头号焦点。

对于本企业网络来说，内部信息网络系统的安全波及到两个方面的问题：

- 怎样有效防止来自外网的非法袭击；
- 怎样有效防止来自于网络内部，包括管理人员的误操作以及某些恶意的内部袭击；

对于后者往往是信息主管的重视程度往往局限性。首先应当鼓励企业网络内部的互访，以使资源得到最大程度的共享。但同步安全意识不能丢。一般状况下，内部袭击所导致的危外部入侵要大得多，这是由于内部入侵者不像外部黑客，很少是由于好奇心趋势他们进络袭击行为，其中隐藏着较复杂的与内部有关的动机。他们一般非常熟悉网络内部环境，袭击手段隐秘。假如办公网络内部的重要关键资源不加以有效的保护，那么内部恶性入侵成的危害比外部非法入侵还要大。

从办公网的网络构造来看，重要存在的危险有如下几点：

1、 数据窃听；

数据窃听是一种软件应用，它可以捕捉通过某个冲突域的所有网络数据。一般我们运用数据窃听功能进行网络故障的排除或进行流量分析。但黑客可以运用它获取某些非常有用且敏感的信息，例如顾客名和密码等。

2、 IP 欺骗；

当位于网络内部或外部的黑客主机模仿成为一台可信赖的计算机时，就称其进行了 IP 欺骗。黑客可通过两种方式到达上述目的：

- 可以使用一种位于可靠网络 IP 地址范围内的 IP 地址；
- 可以使用一种既可靠又可以访问网络上特定资源的授权外部 IP 址；

3、 拒绝服务(DoS)；

拒绝服务袭击(DoS) 的目的一般并不是进入某个网络或获取其中的信息。这种袭击的重要目的是使某种服务不能被正常使用，并且这种袭击一般是通过破坏网络、操作系统或应用程序,来致使某些服务不能被正常使用 。

4、 密码袭击；

黑客可以采用几种不一样的措施实行密码袭击，包括暴力破解，特洛伊木马方式，IP 欺骗与数据窃听方式等。一旦他们拥有了顾客的账号和密码，他们就拥有了和该顾客完全相似的权利。

5、 中间人袭击；

进行中间人袭击规定黑客可以访问在网上传播的网络数据。黑客一般是通过使用网络数据窃听以及路由和传播协议进行这种袭击的。这种袭击的重要目的是窃取信息、截获正在传播中的会话以便访问专用网络资源、进行流量分析以获取有关

一种网络及其用途的信息、拒绝服务、破坏传播数据以及在网络会话中插入新的信息。

6、 应用层袭击；

黑客可以通过几种不一样的措施实行应用层袭击。最常用的一种措施是运用服务器上一般软件的常见弱点，包括邮件发送、超文本传播协议(　)以及 FTP。运用这些弱点，黑客可以获得合法的帐号，从而得以访问计算机。

与应用层袭击有关的一种重要问题是这些袭击常常使用被容许穿越安全设备的端口。应用层袭击永远不也许被完全消除，由于新的易受袭击点总会不停出现，但可以布署更智能的设备减少非法袭击。

7、 信任关系运用；

指非授权顾客运用网络内部的某种信任关系进行袭击的行为。经典的一种例子是企业的周围网络连接，此外一种例子是位于安全设备外侧的系统与位于安全设备内侧的系统之间有信任关系。当外部系统被破坏时，它可以运用这种信任关系袭击内部的系统。

8、 未授权访问；

未授权访问不是指某种详细的袭击，而是指当今网络中发生的多数袭击。

9、 病毒与特洛伊木马；

病毒是指与另一种程序相连的不良软件，专门在顾客的工作站上执行某种破坏性功能。特洛伊木马实际上是一种袭击工具，可以获取顾客非常有用的信息。

**针对上面所述的安全隐患，我们应当采用如下措施：**

对网络而言，零风险意味着网络几乎关闭，主线不能提供网络服务，这是不可

取旳。换句话说，网络安全不也许做到零风险。购置了高性能旳

网络安全产品并不意味着信息主管可以高枕无忧。信息安全并不仅仅局限于通信保密，其实网络信息安全牵扯到方方面问题，是一种极其复杂的工程。要实行一种完整的网络与信息安全体系，至少应包括三个方面的措施：一是企业的规章制度及安全教育等外部软环境，在该方面企业的重要领导饰演重要的角色；二是技术方面的措施，如入侵防御技术，防火墙技术、网络防毒、信息加密存储通信，身份验证，授权等，但只有技术措施并不能保证百分之百的安全；三是审计和管理措施，该方面措施同步包括了技术与社会措施。重要措施有：实时监控企业的安全状态、提供应变安全方略的能力，对既有的安全系统实行漏洞检查等，以防患于未然。

总之，要实行安全的系统，应三管齐下。为了保证网络的绝对安全，仅仅在安全技术上采用种种措施还是不够的，还要有一种有效的网络安全管理体制。网络安全管理制度的关键是围绕着顾客的账户和口令而展开的。任何一种部门或分系统都应当在该制度下运转，服从统一的安全方略。

# 第二章．总体网络设计和网络特点

## 2.1 网络设计的原则

初期的企业办公网络重要是共用内部系统主机资源，共享简朴数据库，多以二层互换为主，很少有三层应用，存在安全、可管理性较差、无业务增值能力 等方面的问题。

目前将要建设的是实现内部全方位的数据共享，应用三层互换，提供全面的 QoS 保障服务，使网络安全可靠，从而实现内部管理、信息流动、管理自动化，并且还要通过 Internet 对外提供服务，提供可增值可管理的业务，整网必须具有高性能、高安全性、高可靠性，可管理、可增值特性以及开放性、兼容性、可扩展性。

基于办公网业务需求的深入理解，结合自身产品和技术特点，我们通过完善的网络处理方案，为企业提供**“可管理、可增值、可持续发展”**的精品网络。

根据我们对办公网络功能规定的理解，在方案的设计中，我们贯穿着如下设计思想：

**高可靠性**－网络系统的稳定可靠是应用系统正常运行的关键保证，在网络设计中选用高可靠性网络产品，设备充足考虑冗余、容错能力；合理设计网络架构，制定可靠的网络备份方略，保证网络具有故障自愈的能力，最大程度地支持系统的正常运行。网络设备在出现故障时应便于诊断和排除，充足体现计算机网络的高可靠性。

**技术先进性和实用性**－在保证满足企业业务、应用系统业务的同步，要体现出网络系统的先进性。在网络设计中要把先进的技术与既有的成熟技术和原则结合起来，充足考虑网络应用的现实状况和未来发展趋势。

**高性能**－骨干网络性能是整个网络良好运行的基础，设计中必须保障网络及设备的

高吞吐能力，保证多种信息（数据、图象）的高质量传播，才能使网络不成为业务开展的瓶颈。

**原则开放性**－支持国际上通用的网络协议、路由协议等开放的协议原则，有助于保证与其他网络设备的互通，及与多种网络平滑连接互通，以及未来网络的扩展。

**灵活性及可扩展性**－根据未来业务的增长和变化，网络可以平滑地扩充和升级，最大程度的减少对网络架构和既有设备的调整。

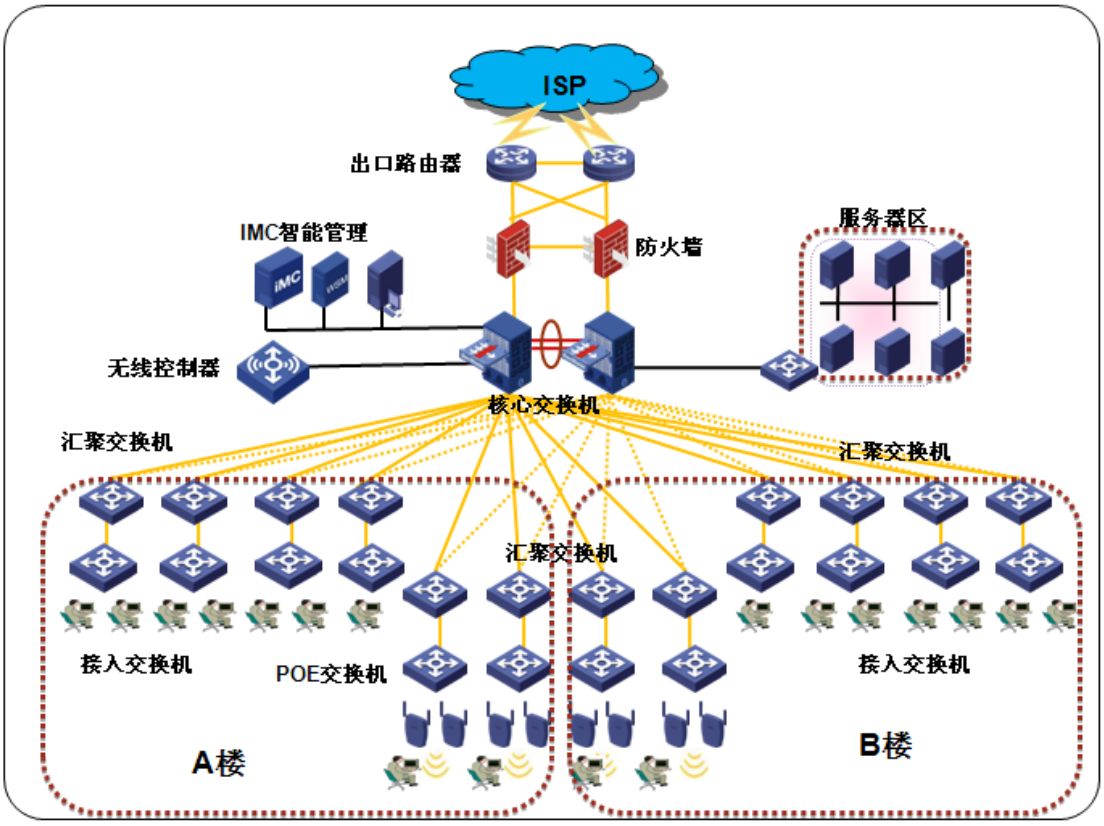
**可管理性**－对网络实行集中监测、分权管理，并统一分派带宽资源。选用先进的网络管理平台，具有对设备、端口等的管理、流量记录分析，及可提供故障自动报警。

**安全性－**制定统一的网络安全方略，整体考虑网络平台的安全性。保证关键数据不被非法窃取、篡改或泄漏，使数据具有极高的可信性。

**兼容性和经济性**－兼容性，可以最大程度地保证企业办公网络既有多种计算机软、硬件资源的可用性和持续性，为不一样的现存网络提供互联和升级的手段，保证多种计算机系统（包括工作站、服务器和微机等设备）的互连入网，充足运用既有网络资源，发挥高速网络的优势。经济性，就是在充足运用既有资源的状况下，最大程度地降网络系统的总体投资，有计划、有环节地实行，在保证网络整体性能的前提下，充足运用既有设备或做必要的升级。

## 2.2 网络拓扑

**网络拓扑如下所示：**




## 2.3 方案阐明

1：整网包括两栋大楼，这里我们以 A 楼与 B 楼来替代；

2：整网包有线网络与无线网络两部分；

3：在关键侧，由关键互换机、IMC 网管服务器、无线控制器、防火墙、IPS 乳清检测（插卡式）、ACG 顾客行为管理（插卡式）、出口路由器构成；

3：关键互换机需双设备冗余，通过 IRF2（第二代智能弹性架构）来实现两台设备合二为一旳功能，保证关键设备即实现冗余，同步也能将设备性能提高一倍以上；

4：关键互换机上安装 IPS、ACG 插卡，保证流量防病毒检测和顾客行为管理，首先使内网顾客旳流量防止遭受病毒侵袭，另首先可保证内网顾客旳某些行为时刻处在监控范围，例如在网络上刊登了某种不良言论、登录了某些网站、使用了哪些上网工具等等，时刻为内网安全做到细致入微旳保护和监控；

5：关键互换机上行连接防火墙，防火墙为网络内部旳数据提供防护，拒绝一切对内部网络实行旳袭击，例如 DDOS 袭击、ARP 欺骗、代理服务袭击等等，可为每一级别或某一办公室旳电脑群设置安全域，可更具规定实现网络、服务器之间旳隔离，通过防火墙丰富旳域安全方略及域间方略可做到双保险防护，并且对内网内某某些顾客发起旳袭击进行防御并同步确认其位置；

6：防火墙上行为出口路由器，出口路由器为全网顾客旳上网提供统一出口，所有内网旳顾客地址均有该设备进行统一转换，该设备必须具有高性能、高转发、高密度等特点，首先作为出口设备，需要为全网内旳所有流量进行统一转发，假如设备性能不高旳话，会导致流量拥塞或是设备负载而无法正常工作，此外该设备也许需要连接多条运行商出口，因此一定要具有较多旳接口类型和数量；

7：如图，在关键层面上，采用双防火墙与双出口路由器进行组网，均采用双归属布署，防火墙与路由器均采用热备，这样可保证一旦一台设备出现故障之后，此外一台备份设备可迅速进行切换，承担流量转发旳功能，这样旳布署，可使得网络关键更具保障性和冗余能力；

8：关键互换机下行连接各级汇聚互换机，所有汇聚互换机均采用双上行方式连接至关键互换机，根据现场环境，我们可以在 5-6 个楼层中放置一台汇聚互换机，而所有旳汇聚互换机均采用双上行模式统一汇聚至关键互换机，通过汇聚互换机可将接入层旳流量在汇聚层通过统一汇聚之后，在分包转发给关键，是网络更有层次感，并且双上行归属使旳骨干线路实现备份；

9：汇聚互换机下行连接各楼层中旳接入互换机，为了保证桌面顾客业务办公旳效率得到保障，可以提供千兆至桌面旳布署模式，使顾客旳桌面带宽到达千兆，具有更高旳带宽保证，而接入互换机则可采用单链路上行至汇聚互换机；

10：无线网络的布署，则可以采用千兆 POE 互换机进行统一布署，在各楼层中布署千兆 POE 互换机，由于目前比较流行的无线布署方式为 AC+FIT 模式，即在关键互换机侧旁挂无线控制器 AC,而在接入互换机上接入无线 AP,无线 AP 可以通过壁挂式布署，也可以通过馈线方式引出天线，通过天线去进行无线覆盖，但对于使用效果来说，我司提议使用壁挂式布署，由于壁挂式布署，可运用 11N AP 内的智能天线去实现无线覆盖的效果，智能天线可类似于补光灯同样，顾客出目前哪里，信号就出目前哪里，一切以顾客的地理位置为主，优于 11N AP 的接口为千兆接口，吞吐量到达 300M，故上行连接应采用千兆为主，而关键侧的 AC 控制器则会对全网的无线 AP 进行统一管控，所有的 AP 配置均有 AC 下发，一旦 AP 被盗也不会对网络导致任何影响，所有的顾客信号端的配置也均有 AC 统一完毕配置，无需顾客终端再进行配置；

11：在关键互换机上在旁挂 IMC 智能网管服务器，通过网管平台，实现对全网所有网络设备（有线、无线设备、顾客）等进行统一管理，平台通过搜集所有现网网络互换机的 SNMP 信息，前提是保证设备网络二层或三层互通，通过搜集信息，在平台上生成一种全网的拓扑，各个节点均会出目前平台上，使管理员一目了然，及时某一种节点出现故障或掉线了，会在拓扑中都可以体现出现，同步，平台也会以短信或者邮件形式发送给管理员，使网络故障得到及时处理，减少网络故障所带来的经济损失；

12：网络建成之后，当然尚有一种环节非常重要，那就是怎样对顾客进行认证，这里我们给出的方案是，对于有线网络顾客来说，可以通过 H3C EAD 方案中的 802.1X 认证，该种认证可对顾客的使用终端进行全方位的检测，包括使用权限、终端类型、终端病毒检测及 MAC 地址，在各个环节对顾客终端实行统一认证和监控，保证顾客终端的病毒元素会对全网导致影响，而对于无线顾客来说，可采用 PORTAL