北京地区医院信息系统基础设施

建设指南

2007 年 12 月

北京市公共卫生信息中心

北京地区医院信息化基础建设促进小组

《北京地区医院信息系统基础设施建设指南》

《北京地区医院信息系统基础设施运行与管理规范》

编委会

目录

前　言

当前，医院信息化是医院建设的基础，是医院现代化建设的核心，是医院实现“加强管理、提高质量，优化流程、方便病人，控制成本、降低费用”的重要和有效手段，是区域卫生信息化建设的重要内容，是保证公共卫生信息系统良好运行的有力支撑。北京地区经过了二十多年的医院信息化历程，在这一历程中，政府和老百姓对改善医疗服务质量和水平的要求更加强烈，其他行业在信息化方面的成效愈加显著，特别是经历了 2003 年抗击非典的斗争，越来越多的卫生行政部门和医院管理者、卫生信息化工作人员更加清晰地认识到信息化对医院发展的重要性，对区域卫生事业发展的重要性，对满足老百姓不同层次卫生服务需求的重要性。

医院信息化建设内容庞杂，是一项非常复杂的建设和管理的系统工程，而要提高整个北京地区医疗机构的信息化水平更是一项非常艰巨的任务。北京地区有各级各类医疗机构 5903 家，还有 2834 多家村卫生室，是全国医疗卫生资源最丰富的地区。这些医疗机构不仅在规模、水平上极富差距，还隶属于不同的主管部门或实际拥有者，在信息化建设的投入、效果上也差异显著。不仅如此，医院的信息化建设还普遍面临着资金、人才、标准等难题，以及一些更为具体的困惑，如：医院信息系统的建设工作在医院如何组织，如何实施，如何保障？医院信息系统建设涵盖的内容，如何按照统一的框架结构作好整体规划？如何作好医院信息系统的运行、维护和管理？有没有统一的流程和制度？已运行的医院信息系统运行状态，按照何标准检测系统运行状况和进行安全评估？如何把风险降到最低？

这些问题在各医院信息化的实践中更为现实、具体、普遍。为统筹协调北京地区医院信息化建设，发挥北京地区专家资源的优势，为各医院的信息化建设提供支持，实现对医院信息化建设的管理、运行实现规范化和标准化。在北京市公共卫生信息中心的具体组织下，北京市卫生局成立了促进北京地区医院信息化基础建设专家小组，开展了《北京地区医院信息系统基础设施运行与管理规范》（以下简称《规范》）和《北京地区医院信息系统基础设施建设指南》（以下简称《指南》）的编制工作。

在编制过程中，专家组认真学习我国有关计算机信息系统的法规和制度，如《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际互联网管理暂行规定》、《中华人民共和国互联网安全保护技术措施规定》（公安部令第 82 号）、《信息产业部信息系统安全等级保护条例》、《卫生部医院信息系统基本功能规范》、《国家中医药管理局中医医院信息化建设基本规范》、《北京市公共服务网络与信息系统安全管理规定》等，力图使上述法规和制度在《规范》和《指南》中得到充分的贯彻和落实。同时，专家们花费了大量的时间去了解和把握国际信息技术管理业务的发展趋势，充分学习和借鉴了 ISO/IEC20000、ISO17799、ISO27001、ITIL 等国际先进的标准和理念，并结合北京地区医院信息化建设的实际情况，努力使医院信息系统建设和管理符合国际标准化质量管理体系。

《指南》和《规范》各有不同的侧重，《指南》侧重于信息系统基础设施规划和建设的技术层面，《规范》侧重于信息系统基础设施的管理和运行维护层面，二者在内容上是相互对应的。

《指南》按照信息系统基础设施内在的逻辑层次分为四个部分，包括网络系统、基础服务、网络布线系统、机房环境建设；共七章，包括医院信息系统基础设施建设的规划、网络系统规划与设计、网络基础服务、网络系统建设、网络安全管理、网络布线系统、机房建设及相关标准。把国际相关标准与北京地区医院的基本情况相结合是《指南》内容编写的基本原则。

《规范》的内容由组织管理体系、规划与计划、规章制度、运行管理、操作规程、信息系统、突发事件应对管理等章节组成。明确了信息系统管理的组织机构和职责，制定了信息系统运行和维护的相关规章制度，优化了信息系统的管理流程，提供了信息安全的保障措施。

《指南》和《规范》适用于北京地区医院计算机通信网络、信息化基础设施应用工程系统、计算机软件等设计、安装、运行和维护，各种数据库应用和信息服务业的规范化，以及主要信息产品开发与应用的规范化，也为从事医院 IT 服务的厂商、设备供应商提供了服务标准和执行依据。《指南》和《规范》的完成，无疑将为北京市卫生系统作好信息应用工程的统一监督与管理，推进医院信息系统的质量监督和认证工作等奠定重要的技术基础。同时，也可供从事信息化的科

技与管理人员以及信息技术教学人员参考。

在编制过程中，专家与业内同行们越来越认识到《指南》和《规范》对加强医院信息系统建设和管理的重要性，在专家们各自所在医院的积极支持下，在信息中心的组织下，在部分 IT 企业的支持下，专家们分工合作，认真讨论，编制过程中共组织各类专题会 19 次，培训班 3 次，专家参与人 156 次，经过近一年的努力，最终完成了《指南》和《规范》的编制工作。

《指南》和《规范》发布的意义在于：遵循我国及国际标准，初步建立起北京地区医院信息系统的建设规范和医院信息系统服务管理规范，为构建医院信息系统的安全体系结构，细化和落实北京市卫生局开展的“人民满意医院”的评审，提升医院信息系统的整体保障能力和服务水平提供了重要的依据，为今后开展和实施医院信息服务的质量管理认证工作打下了基础。

《指南》、《规范》出台后，北京市卫生局将结合医院管理评审等工作，抓好《指南》、《规范》的宣传、贯彻。同时，在应用的过程中要针对发现的问题加以改进，针对仍有争议的问题加以验证，使《指南》和《规范》在实践中不断完善，并尝试建立起支持医院信息化基础建设规范化的专门机构和队伍，以此促进北京地区医院信息化工作在基础设施方面建立起标准规范和标准架构，实现与国际标准技术接轨，推进北京地区医院信息化工作在建设、管理、运行、维护和服务等方面全面、高效、扎实的开展。

在《指南》和《规范》任务提出和完成的整个过程中，相继得到了多家厂商、集成商的大力支持及技术方面的指导与帮助；北京市公共卫生信息中心为《指南》和《规范》的顺利编制提供了组织和工作上的保证；在《指南》和《规范》编辑过程中，先后得到了局领导及各界专家的热情支持和具体指导。在此一并表示感谢！

《指南》和《规范》的编制规模大，专业技术协调、组织工作多，编制时间紧，工作中难免出现不足之处，敬请读者指正。

北京地区医院信息化基础建设促进小组

适用范围

本指南为筹划、实施、维护和改进信息安全管理建立了指导方针和总体原则。本标准中概括出的对象对信息安全管理的目标提供了通用的指南。

本标准期望实现的控制目标和控制手段是为了满足有风险评估而确定的需求。该标准可作为制定组织安全的实践指南和有效的安全管理实践，有助于建立起组织间活动的信心。

本指南的适用范围包括：

1．卫生主管部门

提供考察医院信息化状况的思路和评价参考，辅助管理业务。

2．医院主管领导

协助制定医院信息化战略，如 IT 规划、建设与管理的宏观架构。

3．工程技术人员

了解并掌握医院信息系统基础设施建设的规划方法和相关技术的应用。

4．服务提供商、集成商、厂商

了解医院应用需求和技术系统的特点，为医院提供具有针对性的产品、方案及服务。

术语与定义

1．IP 地址动态分配

根据用户的请求网络基本服务系统把 IP 地址及相关参数自动分配给用户或回收的一种方式，是提高网络可管理性的重要手段之一。

2．IP 地址静态分配

手工为每台计算机分配一个固定的 IP 地址，明确其网关和子网掩码等 IP 协议参数的网络管理方式。

3．安全策略

在组织中为了对包括敏感信息的资产进行管理、保护以及分发所制定的规则、指导和实践。

4．不可抵赖性

在信息交互过程中，确信参与者的真实性及所有参与者都不可能否认或抵赖曾经完成的操作和承诺。

5．风险评估

分析确定风险的过程。风险评估对信息的可用性、完整性、保密性遭到破坏的概率和对特定系统以及整个医院产生的影响的综合评价。

6．基础设施

支撑医院应用信息系统运行的网络、软件、硬件、环境及管理流程、制度、人员等的总和。

7．机密性

保证只有授权用户才能获得访问资源的权力。

8．可管理性

一个可管理的网络应该具有以下属性：对网络资源集中式管理，易于配置和维护，易于故障排查，易于对用户的管理与控制。

9．可靠性

保持所需行为和结果一致的性质。

10．可扩展性

能够适应医院业务和规模的发展变化，在保持稳定性的前提下，网络系统也要平稳地可持续发展。网络规划的扩展性主要体现在拓扑

结构、IP 地址分配和新技术、新产品的适时采用等方面。

11．可用性

允许授权实体能够按照需求进行访问和使用的性质。

12．内网

未接入 Internet，运行医院的核心业务，安全级别相对较高的网络或网段。

13．事件

没有包含在标准运作之内，并且导致（或可能导致）中断服务或降低服务质量的意外情况或突发情况。

14．突发事件

突然发生的、造成（或可能造成）信息系统不能正常运行的事件。

15．拓扑结构

网络中各个资源相互链接的形式，即网络中网络设备（包括交换机、路由器、服务器等）的位置和几何链接形状。

16．外网

与 Internet 互联，运行医院的非核心业务，安全级别相对较低的网络或网段。

17．完整性

保证资产准确和完整的属性。

18．稳定性

与通常概念的稳定性不同，在本文件中稳定性是指基础服务系统和网络拓扑结构的稳定，网络建立后，网络的拓扑结构应在 3~5 年或更长时间内保持基本不变。包括网络的物理拓扑、逻辑拓扑、IP 地址规划以及各种网络服务等。

19．消失

现象不再出现。

20．信息安全

保持信息的机密性、完整性、可用性；另外，还包含真实性、责任性、不可抵赖和可靠性等。

21．用户

所有接入网络、使用网络资源及提供服务的实体。

22．资产

所有对医院有价值的事物。

23．责任性

指保证一个实体的行为可以追查到责任者的性质。

24．真实性

保证主体或资源的身份与所声明的相同。真实性适用于用户、过程、系统和信息这样的实体。

1 医院信息系统基础设施建设的规划

1.1 概述

医院信息系统作为医院运营的基础保障和医院管理的重要手段，对提高医院管理时效，推动医院管理体制的创新，促进医院管理科学化的进程起到了重要的作用，是医院现代化管理水平的重要标志之一。但是，目前医院信息系统建设还不能完全满足医院运营与管理的需要，其中医院信息系统基础设施建设滞后是影响医院信息系统的重要原因之一。

基础设施是医院信息系统的重要组成部分，基础设施规划是医院信息系统规划的内容之一。

首先，两者规划的依据是医院发展的长远目标、战略规划及用户的需求。制定基础设施规划要遵从法律法规、相关标准和规范的要求，技术方案和产品选型不但满足相关技术指标，还要符合相关法律、法规及规范。

其次，为保证医院信息系统的可持续发展，制定基础设施规划应以建立组织、管理和技术三大框架为原则，在各种技术方案中应充分体现基础设施在今后运行中的可管理性。

第三，基础设施的功能规划设计依据可直接从信息系统对基础设施的功能需求导出。与医院信息系统规划不同，基础设施更直接地受到信息系统在技术层面的要求，基础设施的规划是把这一要求进一步分解落实为具体方案的过程。

第四，基础设施的规划还受到医院安全策略的约束，风险分析是制定基础设施规划的必要步骤和内容。

1.2 规划原则

1.2.1 统一规划、分步实施原则

基础设施的规划要同信息系统的规划统一进行；不同区域、不同应用的需求要统一考虑。根据医院业务需求发展的进程分阶段逐步实施。

1.2.2 完整性原则

规划的范围要完整，规划的层面要完整，参照的标准要全面。

1.2.3 需求驱动原则

功能的设置要针对医院的实际需求而定，避免为技术而技术的做法，提高投入产出比。

1.2.4 实用性原则

目标系统必须具有良好的可操作性和可维护性，能够使操作人员通过全面的系统培训迅速掌握。

1.2.5 可扩展性原则

基础设施的生命周期相对较长，规划时要充分考虑目标系统容量的可扩展性。

1.2.6 持续改进原则

业务需求的变化、新系统的上线、安全策略的改变均会影响对基础设施的要求，规划方案应随需求的变化而改变。

1.3 规划内容

基础设施规划不仅要考虑技术层面的实现，还应考虑配套的组织机构和管理机制的建设。在基础设施规划过程中，应该建立起组织、管理和技术三大框架。

本指南仅涉及网络系统和机房的相关内容，组织机构和管理机制的相关内容请参见《北京地区医院信息系统基础设施运行与管理规范》，应用系统相关的建设及安全问题应按照卫生部《医院信息系统基本功能规范》。

本指南所包含内容包括：网络系统、网络基础服务、网络系统建设、网络安全管理、布线系统、机房建设。

2 网络系统规划与设计

2.1 概述

根据基础设施规划的原则与方法，可以将基础设施具体分解为以下技术部分：网络系统、网络服务、布线系统、机房环境与配套设施。

网络系统是医院信息化建设的重要基础设施，是信息系统的基础平台，网络系统的稳定性直接影响到整个医院信息系统的运行。

按照医院应用的特点和发展的整体趋势，医院中的应用属于多种业务的融合，可以大致分为数据、语音、视频、与外界互联等业务。因此，医院网络要支持多业务融合，总体目标是要达到“容量可扩展、用户可识别、业务可区分、质量可控制、网络可管理”。医院网络系统的设计还需满足今后 3～5 年的业务发展。

2.2 规划设计原则与方法

2.2.1 原则

根据信息安全的要求，网络系统在规划和设计阶段至少涉及保密性、可用性和责任性；从技术和网络管理的需求出发，网络的规划还必须考虑网络的稳定性、可管理性、可扩展性、经济性以及易用性。

网络系统的规划原则就是综合考虑这些方面的需求，根据医院的具体情况找到一个平衡点，使得所建立的基础设施不但能够满足医院不同层面的应用需求，而且使得成本效益比达到最优。

2.2.2 方法

与软件系统一样，网络系统的规划与设计也需要自上而下的设计方法，这种设计方法将重点集中于医院的需求与目标上，同时考虑法律、法规和外部环境。

自上而下网络设计首先要求弄清医院的战略目标和业务需求以

及来自各个层面的约束，然后将这些需求和限制条件落实到技术方案，最后进行实施。

总之，应用需求决定技术方案，技术方案要满足业务当前的需求和近期的发展，如图 2-1。

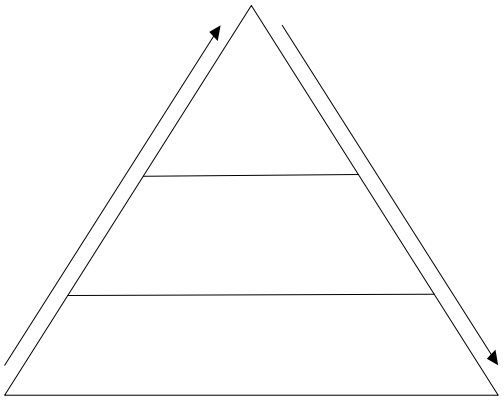

图 2-1

2.3 规划内容

网络是一个复杂的系统，不能把它看成是仅由线缆、交换机、路由器、服务器、桌面 PC 等硬件设备进行的简单互联。它还包括软件、服务、完整的文档以及人的管理。因此，网络规划所涉及的内容至少包括以下几方面：

1．需求调研

2．功能设计

3．逻辑拓扑结构设计

4．物理拓扑结构设计

5．IP 地址规划

6．布线系统设计

7．用户及桌面系统管理规划

8．病毒防治体系规划

9．网络基本服务规划

技术方案对业务目标的支持

战略
业务

网络
网络

网络布线、

10．网络管理与运行规划

2.4 需求调研

2.4.1 需求分析

需求分析是网络规划的基础，应包括以下要素：

1．医院情况

不同规模的医院对网络的稳定性和扩展性要求有所不同。医院的规模决定规划的深度，决定所采用的技术方案以及投资规模。

2．业务需求

业务需求包括：1) 分析应用系统及用户的种类和分布，以确定服务器群的规模，分析流量以确定网络的带宽；2) 明确各种应用系统对安全性的要求；3) 分析组织机构的形式以确定网络的管理模式；4) 分析对外业务交流以确定与医院网络的出口结构。

在对容量的确定上一定要有充分预留。

3．组织结构、院区楼宇及科室分布

分析医院的组织结构以确定网络的核心节点。

分析院区的地理分布以确定网络规模的大小及汇聚节点所在的地理位置。

4．现有网络基础情况

分析现有网络基础是为了确定哪些基础设施（包括硬件、软件和文档）可以继续延用，目的是保护前期的投资。包括：网络拓扑结构、网络 IP 地址、VLAN 划分及使用情况、各设备间情况、布线情况、网络设备情况、应用系统和用户基本信息。

2.4.2 风险评估

风险评估是医院制定安全策略的基本依据，安全策略直接影响到

网络系统的设计方案与产品的选择。在网络规划、设计时要考虑如何规避、转移或降低风险，并平衡方案和产品的投入与风险，网络规划、设计方案应使风险降低到一个可接受的水平。

2.5 网络系统的功能设计

网络功能设计的目的是从应用需求出发分解出网络在技术层面所要实现的基本功能。包括：

1．内、外网是否物理分开

2．子网的结构

3．访问控制逻辑

4．服务器群接口位置与方式

5．IP 地址架构

6．DHCP 部署方式

7．与外界的互联接口位置与方式

8．网络认证中心的设置

9．用户的管理与控制方式

10．时间服务器的部署方式

上述内容将在后续的不同章节进行逐一论述

2.6 内、外网是否实施物理隔离

是否对内、外网实施物理隔离取决于医院制定的安全策略。需指出的是：对内、外网实施物理隔离限制了网络为医院业务提供服务的能力。

本指南对网络的规划与设计是以内、外网作为一个整体考虑的，这主要是考虑到无论内、外网是否实施物理隔离，在规划设计阶段都必须一同考虑，只是在实施时分别部署。

2.7 逻辑拓扑结构设计

2.7.1 概述

拓扑结构体现物理布局和逻辑特征，因此，拓扑结构又分为物理拓扑和逻辑拓扑。网络的逻辑设计对网络的性能、可管理性和扩展性产生直接影响。

逻辑拓扑设计主要包括虚拟局域网（VLAN）的划分及其之间的访问控制逻辑、IP 地址规划、路由规划以及各种网络服务的部署方案。

2.7.2 网络拓扑的层次结构

网络的层次结构是指网络系统功能的分层部署。通常将网络功能分为三层：核心层、汇聚层和接入层。根据实际情况，有时也可分为二层：核心层和接入层。

二层的网络，一般是交换网络，或称为二层交换网络。三层的网络，则多是路由网络，也称为 IP 交换网络或三层交换网络。

通常情况下，功能在各层的分配情况如下：

核心层　迅速转发数据包

汇接层　隔离网络拓扑的变化
控制路由表的大小
数据流的汇聚

接入层　接入数据流
访问控制
执行其他边界功能

各层上交换机的性能和功能有所不同。核心层和汇聚层交换机必须具有路由功能，即三层交换机，接入层交换机则多为二层交换机。

层次化的拓扑结构具有较好的稳定性和可管理性，易于故障定位和隔离。三层结构的网络有更多的控制手段。

2.7.3 虚拟局域网的规划

2.7.3.1 概述

VLAN 在医院的网络环境中多是以 VLAN 的形式出现，因此，在进行子网规划时实际上就是对 VLAN 的规划。在以后的章节中子网和 VLAN 将表示同一概念。

VLAN 一般部署在接入层，用于逻辑隔离不同用户组，实施访问控制，也常用于设备管理和设备互联。VLAN 的另外一个重要作用就是缩小网络广播域，提高网络的稳定性和可管理性，降低病毒对网络的影响。应避免建立跨越网络核心的 VLAN。

2.7.3.2 VLAN 的规划原则

1．单一化原则

VLAN 中所包含主机的用途尽量单一，以便于管理和实施访问控制。

2．边缘化原则

除了用于接口目的的VLAN外，VLAN应尽量部署在网络的边缘，避免越层，更不能跨越核心，以减少 VLAN 间的相互影响。

3．最少化原则

本原则包含两方面的含义：1）在满足应用需求的前提下，VLAN 的数量越少越好；2）在同一交换机中 VLAN 的数量越少越好。

2.7.3.3 VLAN 的规划内容

1．VLAN 容量规划

VLAN 的容量一般以每个子网不超过 200 台计算机为宜。

当同一汇聚下的同一应用（或部门）的主机数量过多时，可为该应用（或部门）增设第二个 VLAN。两个子网应在不同的物理空间，

不要在空间上有交叉。

2．VLAN 类型选择

VLAN 的划分常基于端口的方式。

3．VLAN 与 IP 地址的关联

为了便于使用，需要在 VLAN 与 IP 地址之间建立关联。对于用户所在的 VLAN，可以为每个子网分配一个 C 类地址大小的 IP 地址段，并明确子网的网关、掩码和用户可用的地址范围。如果是设备互联 VLAN 或者管理 VLAN，可根据实际情况确定网关和掩码。

4．VLAN ID 与名称命名

VLAN ID 与名称应该赋予一些实际意义，以便于记忆和管理，VLAN ID 应预留足够的编码空间为将来以备扩展使用。

2.7.3.4 VLAN 间的访问控制

VLAN 间的访问控制涉及两个问题：

1．控制方式

对 VLAN 间的访问控制手段一般有两种：

1） 通过设置访问控制列表（ACL）；

2）在三层交换的网络中可通过对路由的调整来实现 VLAN 间的访问控制。

另外，在某些产品中可通过访问策略进行控制。

2．控制点的位置

控制点的位置受网络层次结构的直接影响。控制点大都设置在 VLAN 网关所在的交换机上。

2.7.4 路由规划

路由规划要保证路由与网络拓扑结构和 IP 地址分配架构相匹配，能够清晰地识别出拓扑结构的各个组成部分。

2.7.4.1 规划的原则

路由规划的目的是使网络的流量均衡并能灵活调整流量，提高链路利用率。路由规划中要将流量大的用户或网段尽可能分配在不同的路由上。

路由规划要做到：控制路由表的大小，对路由要有良好的控制能力，在出现网络故障情况时路由收敛时间短，从而提高网络的稳定性。具体原则如下：

1．稳定性原则

通过选择恰当的路由策略，合理地划分路由域，可以有效地避免因路由反复变化所造成的系统资源及网络资源的浪费。

2．高效、简洁原则

IP 网络自愈的时间通常取决于网络的大小，即链路数目、节点数目和路由的数目。恰当地选择路由协议，可达到支持快速收敛、网络资源占用少、设备配置简洁等目的。

网络设备的系统软件的版本应尽量统一，避免软件的不一致带来的软故障。

2.7.4.2 规划的内容

路由规划的内容包括：路由协议和路由策略的确定、网络内部和网络出口的路由规划。

1．选择路由协议

静态和动态路由协议有着不同的特点和优点，在具体规划时要根据它们的特点和实际环境进行选择。

通常在网络内部可采用动态路由协议，在网络出口处采用静态路由协议。

2．制定路由策略

制定路由策略的目的，首先是确定静态路由和动态路由在网络中作用的范围和配置的节点，以及路由器间路由信息的发布与接收原则；其次是明确业务应用系统 VLAN 之间的访问控制要求，并通过路由控制实现安全策略。

静态路由的路由策略是由静态路由设置本身直接实现的。而动态路由的路由策略则通过将匹配规则应用于路由的发布、接收和引入等过程得以实现。

3．路由的规划

对于层次结构的网络，路由的划分一般要与其层次结构相适应。在此基础上再考虑业务连续性的要求，使数据流经过的路径尽量短；并且要使网络中的路由能够动态地感知网络的状态，如流量、速率、负载、处理能力和延迟等。

4．对外接口的路由

对外接口的路由规划要解决两个方面的问题：一是外网路由如何导入内网；二是根据业务的访问控制需求确定内网的哪些子网可以访问外网。

一般采用静态路由或缺省路由的方式把外部路由导入到医院的局域网。

2.8 物理拓扑设计

2.8.1 概述

物理拓扑结构规划是通过物理设备、物理链路对网络的逻辑拓扑

进行实例化的过程。包括容量规划、层次结构划分、对外互联接口等。

2.8.2 物理拓扑结构规划的原则

物理拓扑设计的思路是在保证网络层次化的同时实现网络扁平化，以用户分布和流量分布为依据，内外网整体考虑。网络规划的原则是：

1．核心稳定原则

网络的核心层是网络系统的中枢，必须保持稳定。

2．一致性原则

物理拓扑结构尽量与逻辑拓扑结构一致，且与用户及资源的分布匹配。

3．单一出口原则

尽可能将所有对外互联的出口进行统一管理，设置统一策略，至少要在同一物理位置上避免出现多个出口、多种策略。

4．均衡原则

在满足应用需求的情况下，应尽量保持网络中各节点流量的均衡，避免偏载。

2.8.3 规划内容

2.8.3.1 网络容量规划

为了确保网络有足够的处理、接入和管理能力，应当考虑业务系统的容量需求，并对未来网络功能和性能的容量需求做出预测。其内容包括：主干带宽，接入带宽，网络设备 CPU 和内存的负载，数据转发速率，网络延迟。

对网络容量的规划还涉及网络的布线系统、逻辑拓扑结构和设备选型。

2.8.3.2 网络设备的互联

在进行网络设备互联时要考虑如下问题：

1．核心层和汇聚层节点数量的确定

1） 核心层节点数量的确定

通常核心节点的数量至少两个，以保证核心区域设备和链路的冗余，视实际情况适当增加。例如，在较大的分支机构和距服务器群较远且用户群集中的区域可考虑增设额外核心接点。

2） 汇聚层节点数量的确定

汇聚节点一般是业务的汇聚点、用户的汇集点或楼宇相对集中的地点，汇聚节点多以楼宇为基础进行设置。汇聚节点的选择也要考虑接入层设备的均衡。另外，对特殊的应用区域（如放射科、超声科）可考虑增加汇聚节点。

3） 每个核心节点链接汇聚节点数量的确定

在重点保障的前提下，每个核心节点要均衡地链接汇聚节点，以实现网络负载的均衡。

2．互联方式

在层次化的网络中主要存在如下三种互联方式：

1） 核心层之间的互联方式

核心层设备之间的互联必须采用冗余技术，包括链路冗余、板卡冗余和机箱冗余，已实现核心层节点间的路由冗余。

2） 核心层与汇聚层的互联方式

核心节点与汇聚节点的互联也应采用冗余技术，包括链路冗余和模块冗余，以避免汇聚层的单故障点设备和链路。在三层交换网络中的目的是增加汇聚层的冗余路由。

3） 汇聚层与接入层的互联方式

汇聚层与接入层的互联一般采用单链路，也可考虑双链路。但在

接入层引入过多的链路会增加网络的复杂性。

对于要求带宽较高的用户（如放射科的读片室）所链接的交换机的上联可采取链路聚合技术，以增加互联带宽。在这种情况下应尽量避免采用交换机的堆叠。

3．避免环路

冗余设备和冗余链路的增加使得网络中出现很多物理环路，存在环路的网络无法正常工作，必须在逻辑上消除这些环路。

在构建二层网络时，一般采用生成树（Spanning Tree）技术避免形成环路。

在构建三层网络时，必须认真规划网络的路由，采用动态路由协议（如 RIP、OSPF 等）是有效的方法。

4. 服务器群的接入

服务器群是网络中的信息源、服务源、数据流源。必须明确服务器群的接入方案，且在拓扑结构图中体现。服务器群接入的原则是：

1）就近链接。选择物理上或逻辑上最近的汇聚节点链接相应的服务器群，使信息源尽可能靠近用户。

2）接入方式。必须采用冗余技术，如链路聚合、VRRP 或 SLB。

3）安全防控。服务器群必须位于独立的网段上，以便进行安全设置和管理。

5. 无线接入

无线接入作为有线网络的拓展，基本作用一是利用无线的灵活性和移动性，为医护人员提供随时随地的网络接入服务；二是对医院业务连续性要求高的窗口业务（门诊挂号、收费等）提供网络备份。

在部署无线系统之前，要进行认真的现场调查，以确定 AP 的数量和部署位置。

在进行现场调查的时候，要进行三维调查，不但要考虑位于同一个楼层的 AP 之间的相互作用和影响，还要考虑相邻楼层的 AP 之间的相互作用和影响，以利于 AP 的高效利用和避免同频干扰。

相邻 AP 之间的无线信号覆盖范围要保持 15%~20%的重叠区域，以利于实现无缝漫游功能。

2.8.3.3 对外互联接口的规划

按照目前医院的应用需求，医院网络出口通常有三种类型：一是互联网（Internet）的接入，如与电信运营商及科研教育网的互联；二是与专用网络的互联，如与北京市医保网的互联、与社区医院的互联；三是通过互联网以 VPN 形式建立的与医院分支机构的互联。

对外互联接口的结构依赖于整个网络的拓扑，在二层和三层网络中对外出口的链接位置会不同。对于二层网络，出口一般设置在核心交换机上，而在三层网络中则要设置在汇聚交换机上。但互联接口本身结构的区别并不大。

对外互联结构的规划就是综合考虑应用需求，选择适合的技术方案和措施。

对外互联接口规划的重点在于网络的安全控制与管理。

2.8.3.4 Internet 的接入

在接入 Internet 时，主要考虑以下几个问题：

1．Internet 接入提供商（IAP）的选择

目前，IAP（Internet Access Provider）很多，有不同的级别和不同的价格。大的 IAP，如中国网通和中国电信等，一般都有自己的国际出口，带宽能够得到保障，但价格较贵；小的 IAP 一般是租用大的 IAP 的线路，没有自己的国际出口，但价格便宜，一般只有大 IAP 价格的 1/5~1/6。

2．接入方式

医院接入 Internet 时可考虑如下两种方式：

1）固定的物理链路接入方式

医院应该采用该种方式接入，该方式链路和带宽稳定，有固定的 IP 地址，便于维护和控制。这种方式又有光纤和实缆两种介质形式，医院可根据情况进行选择。

2）ADSL 方式

社区医院可考虑 ADSL 方式接入。在具体实施时可考虑多条 VDSL 捆绑。这种方式价格最便宜，但不适用于大医院。

3．必要条件

在接入 Internet 时，除了与服务商互联的链路外，路由器和防火墙是必需的硬件设备。如果要对上网用户有较强的管理和控制手段，则需建立用户认证系统、流量控制和病毒防护系统。用户认证系统最好设计成全院统一的认证中心。

如果需要从院外访问院内的资源，需要设置 VPN 服务器，还要注册相应的域名，必要时要设置自己的 DNS 服务器。

4．访问控制策略

出口节点既是医院网络的安全边界，显而易见，它又是安全薄弱点。出口的结构设计侧重于安全，同时要兼顾性能，必须要做访问控制。访问控制的目标是保护网络化服务，包括两方面内容：一是保障内网的安全，二是保障对外业务的连续。

策略应包括以下内容：

1）允许访问的网络和网络服务

2）确定允许谁访问哪个网络和哪种网络服务的授权程序

3）用以保护网络链接和网络服务访问的管理控制措施和程序

5．访问控制的方式

1）网络划分

2）网络链接控制

3）网络路由控制

4）网络安全服务

6．多 Internet 出口的处理

很多医院互联网的出口有两个，一是中国网通（CNC），二是中国教育科研网（CERNet）。当有两个出口时，对外互联的结构会变得复杂一些，首先是路由设置的复杂，其次是域名服务器设置的复杂。参见策略路由一节。

需要注意的是，在向 ISP 申请 Internet 接入时要明确说明所需要的 IP 地址数量以及相关网络配置的详细参数，以便于网络的扩展和维护。

2.8.3.5 与医保网的互联

各医院的网络按照医保网的相关规定接入北京市医保网，同样也要实施访问控制。与医保网互联最好与医院网络的其他对外出口（如 Internet）一同考虑，做到统一出口，以方便管理。

2.8.3.6 与社区医院的互联

与社区医院的互联一般采用虚拟专用网络（Virtual Private Network, VPN）技术，通过公共网络把内网扩展到社区医院。在采取 VPN 方式时，也可根据医院与社区业务的紧密程度采用不同的 VPN 形式。

在需要实时或访问频率较高时可采用站点到站点（Site-to-Site）方式的 VPN，否则，可采用远程访问（Remote Access）形式的 VPN。

另外，向电信公司租用一条逻辑链路（如一到数条 E1 链路）也是可行的方案。

2.8.3.7 远程访问

VPN 是通过跨越共享或公共网络的链路而使医院内部网络得到扩展的一种技术。

为支持远程用户访问院内网上的资源，需要在医院网上设立 VPN 环境，这时建立的 VPN 一般属于远程访问（Remote Access）方式。在搭建 VPN 物理环境前需要确定选择哪种隧道协议和怎样的认证系统。

2.8.3.8 对外互联的拓扑图

目前，在一般医院的网络环境中，会选择靠近内网中心的位置作为与外界的链接点。对于二层结构的网络，一般选择核心交换机；对于三层结构的网络则会把链接点放在汇聚层交换机上。如图 2-2、图 2-3 所示。

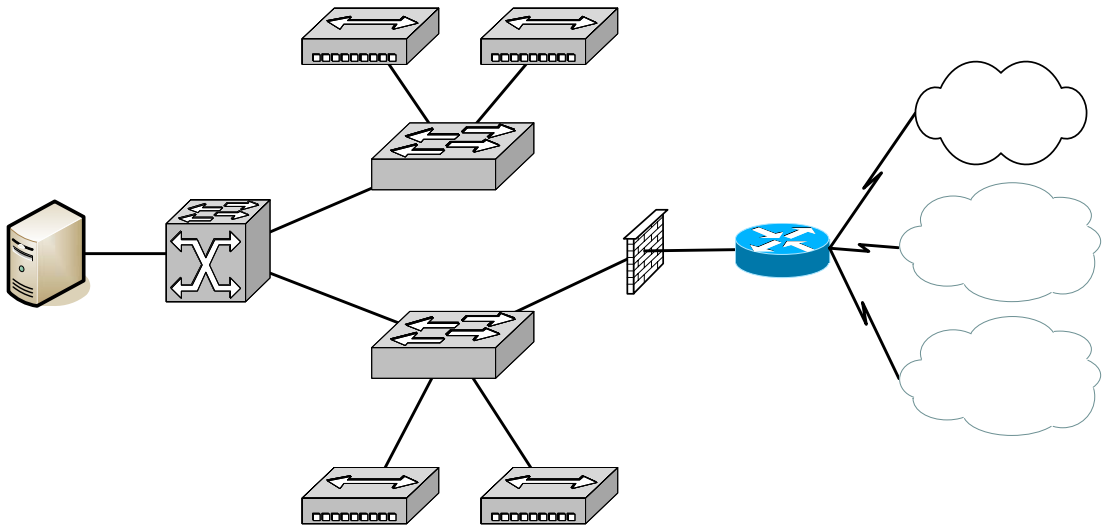

图 2-2 三层网络的链接点在汇聚交换机上

接入层交换机

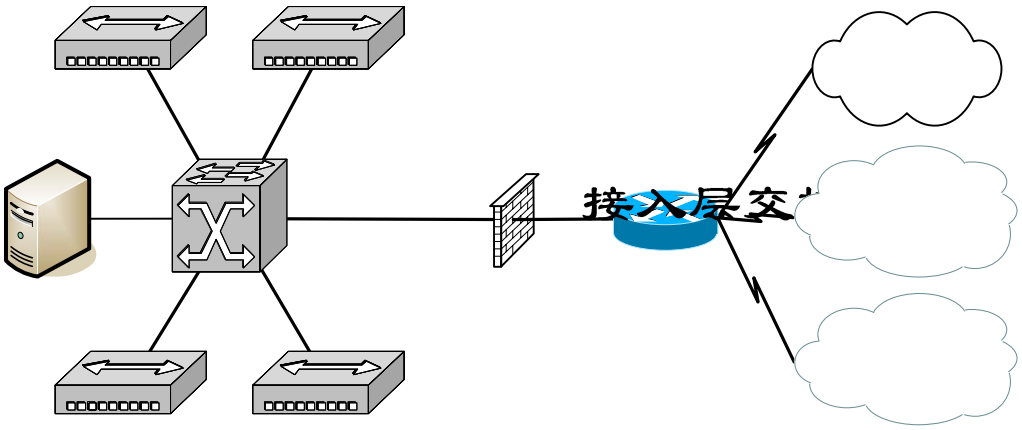

图 2-3 二层网络的链接点在核心交换机上

图 2-2、图 2-3 中是内、外网合一的情况，如果医院的网络是内、外网物理隔离的，设置方法相同，只要分开设置即可。

2.8.3.9 容灾对网络的要求

容灾对网络的要求是能够提供专用、稳定、高带宽的链路。在院区内比较容易满足这种需求，但如果是异地备份（如在相距较远的两个院区）就需要考虑更多的问题。

在考虑容灾时，网络必须解决以下问题：

1．备份的数据流不能影响正常的网络运行；

2．对持续、大流量备份数据的支持；

3．备份数据的远距离传输（如果需要）。

2.9 地址规划

IP 地址规划是网络逻辑规划的重要内容，是影响网络稳定性的关键因素之一。IP 地址规划的好坏，直接影响路由协议算法的效率及网络的性能、管理效率以及可扩展性。

2.9.1 IP 地址规划的原则

1．管理便捷原则

医院的局域网尽量使用私有网络，私有地址段包括：10.0.0.0/8，172.16.0.0/11，192.168.0.0/16。

2．一致性原则

IP 地址架构应该与网络拓扑结构相匹配，做到逻辑拓扑、物理拓扑以及 IP 地址框架相一致。

3．整网原则

各地址空间的大小应是 2 的幂次，便于各种安全策略、路由策略的选择和设置。

4．物理属性优先原则

IP 地址的划分应首先体现网络的物理拓扑属性，再对逻辑拓扑进行区分，并分别以 IP 地址中的不同段进行标识，方便记忆。

5．易用性原则

IP 地址的分配要便于记忆、易于使用。例如，将网关统一设置为每个地址段的第一个或倒数第一个可用地址，比用其他地址更容易记忆和使用。

6．地址预留原则

地址预留是网络系统扩展性和灵活性的基本要求，在网络拓扑变化或应用系统变化的情况下，可以按照既定的规则，给出合适的 IP 地址，体现划分原则的连续性。

2.9.2 IP 地址规划的内容

IP 地址规划至少包括如下内容：

1． IP 地址分配的总体架构

2. 核心层的 IP 地址分配

3. 汇聚层的 IP 地址分配

4. 接入层（终端）的 IP 地址分配

5. 层间互联 IP 地址的分配

6. IP 地址与 VLAN 的关联

7. 设备的 IP 管理地址

2.10 网络管理规划

2.10.1 概述

网络管理是网络运行阶段的主要任务，主要包括技术手段、人员组织及行政管理。建成一个可管理、易于管理的网络必须从网络建设的各个阶段入手，因此，网络管理的规划非常重要。

本节的内容只涉及网络管理技术手段的规划，有关人员组织、行政管理规划的内容请参见《北京地区医院信息系统基础设施运行与管理规范》。

2.10.2 规划的原则

为了提高网络的可管理性应遵循如下原则：网络核心简洁化，访问控制边缘化，网络结构层次化，控制手段多样化，故障影响局部化，管理控制集中化。

2.10.3 规划的内容

网络管理规划在技术层面上包括性能管理规划、故障管理规划、配置管理规划、计费管理规划和安全管理规划等，涉及网络功能、拓扑结构、IP 地址规划、路由规划、用户管理、网络基础服务等内容。

对网络可管理性的考虑应该渗透到各个阶段、各个层面的规划、

设计中。

2.11 IP 地址管理规划

2.11.1 概述

IP 地址管理包括局域网内部 IP 地址管理和外部合法的 IP 地址管理两部分，管理的重点是前者。IP 地址管理已经成为 IT 管理的重要内容，是网络安全管理的组成部分。

医院应当建立健全 IP 地址管理的制度，对 IP 地址的分配使用实行备案管理。

2.11.2 管理方式

IP 地址管理方式包括静态分配和动态分配。服务器及网络设备的 IP 地址采用静态方式分配，客户端 IP 地址可采用动态方式分配，也可采用静态方式分配，但不可并用。

动态分配需架设 DHCP 服务器。若医院网络规模较大，可设置多台 DHCP 服务器以均衡客户端的地址请求。

采用静态方式分配 IP 地址时，对分配的 IP 地址要作授权管理，明确使用人、接入物理位置、链接的设备端口和有效使用时间等。

3 网络基础服务

3.1 概述

为保证网络系统的正常运行，为用户提供网络支持而进行的管理和控制等工作称为网络基础服务。

网络基础服务在完成保障网络运行的同时，还为应用系统与网络系统提供了相互结合的环境和条件，为整个信息系统的安全管理打下了基础。

本章将重点讨论基本网络服务所包含的内容：名字服务（DNS、WINS），DHCP 服务，时间服务（NTP、SNTP），认证服务（RADIUS、Kerberos、LDAP、CA/PKI）。

3.2 名字服务

名字服务的作用是帮助计算机用户把字符串名称翻译成为 IP 地址，以方便用户及系统对网络资源的引用，并屏蔽网络系统环境变更对系统配置的影响。

3.2.1 医院网络环境中的名字服务

在医院网络环境中主要存在两种名字服务：WINS 和 DNS。它们具有各自不同服务机制。

WINS 是微软开发的名字服务系统，是针对 NetBEUI 协议对主机的命名。这种主机的名被称为 NetBIOS 名称。WINS 的作用是将 NetBIOS 名字解析为 IP 地址，WINS 服务主要用于 Windows 2000 以前的版本。

DNS 是被广泛用于 Internet 的名字服务，Internet 对主机的命名称为完全限定域名（FQDN）。DNS 的作用是将 FQDN 名称解析为 IP 地址。FQDN 名称除包括主机名外，还包含主机所在域的名称。

NetBIOS 名字和 DNS 名字，主要区别如下：

	NetBIOS 名字	DNS 名字
类型	平面	层次
组成字符限制	Unicode 字符，数字	A～Z，a～z，0～9 和连字符“-”
最大长度	15 个字符	DNS 域名的每一节最大长度为 63 字节，FQDN 长度最大为 255 字节
名字解析方式	广播 WINS 服务器 Lmhosts 文件	DNS 服务器 Hosts 文件
通讯协议端口	UDP 137	UDP 53

3.2.2 名字服务的规划内容与原则

首先，在医院中明确以下问题：

1．名字服务的选择

2．域名服务器的部署方式

3．域名的确定，包括内部域名和外部域名

4．主机的命名规则

其次，要按照以下原则进行规划：

1．确保安全性，避免内部名字信息不能从外部访问

2．域名服务器的冗余

3．易于扩展，对分院的支持、对科室的支持

3.2.3 名字服务的选择

DNS 服务在医院网络中是必须的服务，对内、对外均需要提供 DNS。WINS 服务的优势是简单易行，维护量极小，对于小而简单的网络可考虑使用。

通常情况下，WINS 和 DNS 同时使用。

3.2.4 WINS 的部署

在 Windows 环境中部署和管理 WINS 都比较简单，但需要注意以下几个问题：

1．WINS 服务的冗余，至少要有两台独立的服务器；

2．WINS 数据的备份；

3．WINS 与 DHCP 相互配合；

4．对不同操作系统的支持（必要时可能需要 Lmhosts 文件的配合）。可用 Windows 域中的域控制器兼任 WINS 服务器。

3.2.5 DNS 的部署

在医院网络环境中，对 DNS 服务的需求有以下几个方面：

1． 内部信息系统运行环境中需要 DNS 支持的服务及系统；

2． 内部客户端程序；

3． 外部用户（提供医院对外服务各种主机的名字解析）。

其中第一种对 DNS 的要求最高、最严格。

DNS 的部署包括：DNS 命名空间、DNS 服务器位置、DNS 分区（Zone）、客户端 DNS 的配置以及内部 DNS 和外部（Internet）DNS 的关系。此外，还要考虑到 DNS 服务的安全性及扩展性。

3.2.5.1 DNS 命名空间

DNS 命名空间就是 DNS 域名及其结构。DNS 域名是以树状结构进行管理的。

医院可以申请一个或多个 Internet 域名，同时也可以在局域网内部创建自己私有的 DNS 命名空间。不过，对于 Internet 而言，这些私有的 DNS 命名空间是不可见的。

要定义局域网内部的 DNS 域名和外部（Internet）域名，并分别进行管理。两者的关系一般有两种情况：

1．将内部域名作为外部域名的子域

2．内、外域名相互独立

前者易于部署和管理，后者安全性较高。

3.2.5.2 DNS 服务器的架构

DNS 服务器存有 DNS 命名空间的信息，并以此来回答 DNS 客户端的请求。DNS 区（Zone）的大小、客户端的数量及位置均对服务器的部署产生影响。

按照作用，DNS 服务器可分为如下几种类型：

1．主 DNS（Primary）服务器：创建了区域的 DNS 服务器，其中的数据是可读可修改的，这是最经常使用的 DNS 服务器。

2．辅助 DNS（Secondary）服务器：不创建区域，其数据是从主 DNS 服务器上复制过来的，数据不能修改。其作用是分担主 DNS 服务器的负担，加快 DNS 解析的速度，以及服务器的冗余。

3．缓存（Cache-Only）服务器：不负责管理任何区域，因此该服务器上没有任何数据，只负责响应客户机查询请求，并将查询到的数据存在缓存（Cache）中。此类 DNS 服务器常用来解决速度较慢的链路上用户的 DNS 请求，例如医院的分支机构。

4．DNS 转发服务器（Forwarder）：将域名请求转发给其他（通常

是外部）DNS 服务器。其作用主要是利用条件转发，为内部用户提供外部域名的解析。使用 DNS 转发服务器可避免内部 DNS 服务器暴露到 Internet，同时可降低网络流量。

为了保证得到正确、稳定的域名服务，需要认真规划上述各种类型服务器的取舍、位置、数量及其关系。

DNS 服务器的数量、类型及其关系，与网络拓扑结构一同构成了 DNS 服务的架构。

3.2.5.3 DNS 的安全

由于最初 DNS 采用的是开放通讯协议，因此，DNS 是易于受到攻击的服务之一。DNS 常受到的攻击有：

1．Footprinting 攻击，即跟踪攻击；

2．拒绝服务（Denial of Service，DoS）攻击；

3．IP 欺骗攻击；

4．重定向攻击。

为避免各种攻击，应注意以下问题：

1．防止任何人从医院外部获得内部的网络信息以及内部 DNS 的命名空间；

2．至少要有 2 台 DNS 服务器，对 DNS 服务器做必要的加固；

3．确保内部 DNS 服务器与 Internet 间没有通讯，至少是没有直接的通讯；

4．对配置了请求转发的 DNS 服务器，要只使用内部 IP 地址；

5．所有 DNS 服务器都要限制区数据传输，只能到特定 IP 地址；

6．在所有的 DNS 服务器上设置访问策略，防止缓存污染；

7．如果是 Windows 环境，所有的 DNS 服务最好运行在域控制器上，并对域控制器实施访问控制，以保证只有指定的人员才能对服务

器实施管理任务。

3.2.6 域名管理

医院在 Internet 上的名称需要进行域名登记。域名的种类包括普通域名和中文域名。

域名的管理主要是外部域名的管理，医院要指定专人对域名进行管理。涉及的问题有以下几个方面：

1．注册域名；

2．域名服务器变化；

3．对外服务的增减；

4．IP 地址变更；

5．增加、减少以及变更域名；

6．其他情况，如注册内容、联系人或联系方式的变更，以及域名的续费等。

3.2.7 DNS 策略解析

对具有两个或两个以上出口的医院需要 DNS 策略解析功能，以实现外部用户只通过距自己最近的端口就可访问院内资源。

3.3 DHCP 服务

DHCP 是一种用于简化主机 IP 配置管理的 IP 标准。通过采用 DHCP 标准，可以使用 DHCP 服务器为网络上启用了 DHCP 的客户端管理动态 IP 地址分配和其他相关配置细节。

3.3.1 DHCP 服务的作用

医院网络中的计算机和其它联网设备，如打印机、IP 电话等，都必须正确配置合法的 IP 地址和其它网络参数才能正常工作。DHCP 降

低了对客户端 IP 地址分配和配置的管理开销及复杂性。通过 DHCP 客户端能够自动且动态地获得 IP 地址及相关配置项参数，实施自动和集中式管理。

DHCP 还能为其他服务功能提供自动化的支持。

3.3.2 DHCP 的规划

对 DHCP 服务的规划要解决以下几个问题：

1．确定 DHCP 服务器的位置；

2．确定 DHCP 服务器的数量；

3．对多 VLAN 环境的支持方式。

3.3.2.1 确定 DHCP 服务器的位置和数量

在大多数医院的网络环境中，只需在网络的核心区域安装一台 DHCP 服务器即可。

为了降低整个网络的流量、缩短客户端的响应时间，有时需要安装多台 DHCP 服务器。如有分院、分支机构或链路薄弱（小带宽联接或链路不够稳定）的区域应放置单独的 DHCP 服务器。

如果设备少，也可考虑采用静态 IP 设置。

3.3.2.2 对多 VLAN 的支持

医院的网络中均存在多个 VLAN，要集中部署 DHCP 服务器，就要求网络中的网关设备支持 DHCP/BOOTP 的中继。

如果所用的网关设备不支持 DHCP/BOOTP 的中继，就需要在每个子网中安装中继代理。如图 3-1 所示。

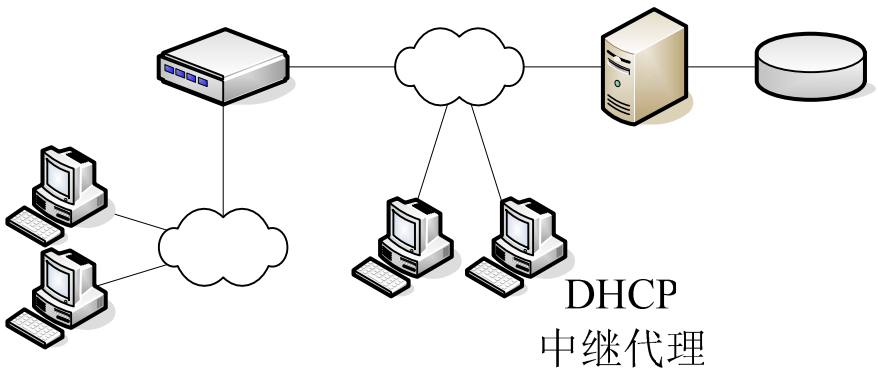

图 3-1 利用 DHCP 中继代理的子网

运行 Windows 2003 的计算机可设置成 DHCP 的中继代理。

3.3.2.3 提高 DHCP 服务的可用性

DHCP 子网-1
客户端

提高可用性的方案需要考虑所有可能出现的故障，包括服务器故障、链路中断和网络设备的故障。可采用以下措施提高 DHCP 服务的可用性：

1．拆分作用域。将 DHCP 的作用域按 80/20 原则分散在两个服务器上。

2．建立 DHCP 服务器集群。利用集群技术增加服务器的冗余，实践中可考虑利用已有的集群服务器。

3．使用 DHCP 备用机。配置一台同样的 DHCP 服务器备用。

4．客户端的措施。利用 Windows XP 或 Vista 中 IP 属性的备用设置可保证客户端总能获得有效的 IP 参数。

3.3.2.4 DHCP 与其他服务的集成

为实现主机名和IP地址的互查，DNS应保持动态的更新（参见3.2.5 DNS的部署），将DHCP与DNS（甚至WINS）相互关联，可使DHCP自动更新获得IP配置的计算机在DNS中相应的资源记录。

3.4 时间服务

在网络环境中时间的同步非常重要，一方面是计费、审计需要准

确的时间，更重要的是网络中一些协议的运行需要更加精确的时间，例如 Kerberos V5 认证协议。

有两种重要的时间同步技术,即利用网络时间协议(NTP 或 SNTP）和直接链接时间传输技术。后者需要所有客户端直接链接到标准时间源。而通过时间协议则可以在一个无序的网络环境下提供精确的时间服务。

3.4.1 时间服务的作用

时间同步的作用如下：

1．网络管理系统的日志审计；

2．应用认证过程；

3．与时间有关的应用系统：IDS/IPS 以及医嘱处理的应用；

4．网络备份系统：在备份服务器和客户机之间进行增量备份要求这两个系统之间的时间同步；

5．计费系统：网络计费系统中也要用到数字时间戳服务，所以也要求精确的时间同步。

3.4.2 时间服务的部署

为保证各设备和系统之间时间的同步，建议采取的措施：一是尽量选取非常精确的时间源；二是将精确的时间传送到需要时间服务的设备或主机，且减小传输过程中的误差；三是选用绝对时间同步的时间设备，充分利用设备的时间校准机制自动实现时间同步，排除人工因素。

不同的网络结构应采取不同的部署方式：

1．内、外网合一的网络结构采用全网统一的时间源服务器，由该时间服务器与外界的标准时间源进行同步。如图 3-2 所示。

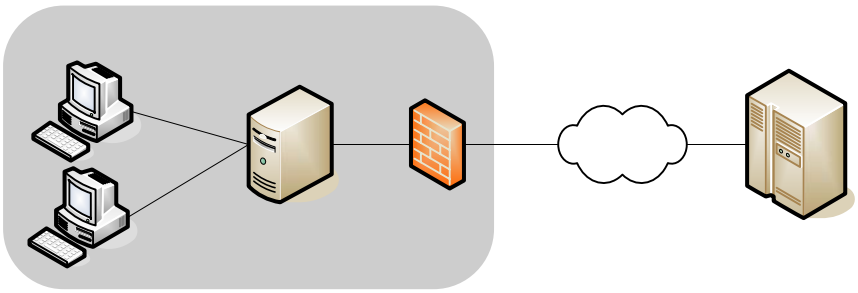

图 3-2 内外网合一时的时间源部署

2．内、外网物理分离的结构只能采用两个时间服务器，分别为内、外网的计算机提供时间服务，但最好利用防火墙将内、外网时间源链接。如图 3-3 所示（外网与内网服务器间用虚线链接）。

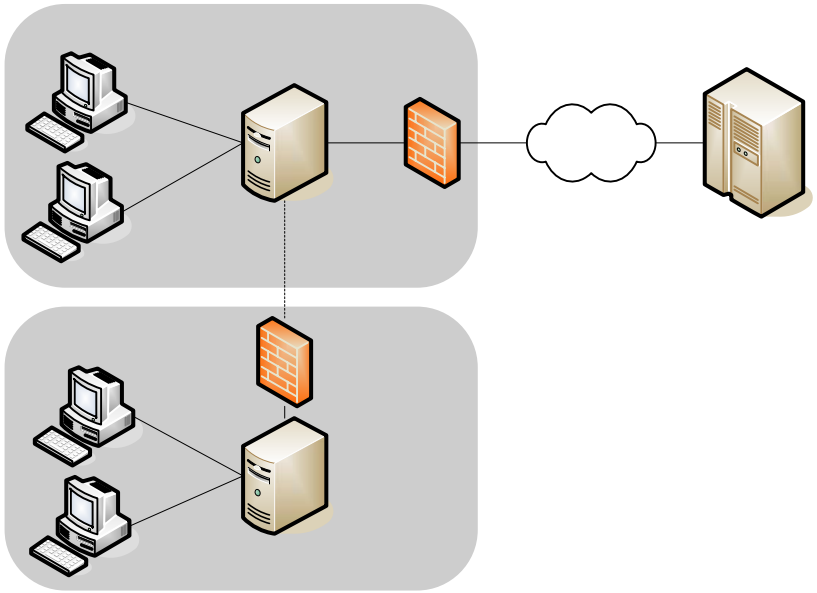

图 3-3 内、外网分离时的时间源部署

3.4.3 时间源的选取

时间同步的实现一般使采用分层结构，不同位置的网络节点会选择不同的时间源，因此时间源的选取是实现时间同步的基础。

对运行 Windows 系统的客户端最好采用 Windows 域管理，域中的客户端会自动以域控制器（DC）作为时间服务器，并自动与之进行时钟同步。

标准时间源应尽量就近。通常可选中国科学院国家授时中心的时间服务器（210.72.145.44）作为标准时间源。有科研教育网（CERNET）

出口的教学医院也可以选择下表中的时间服务器：

主机名	地理位置
s1a.time.edu.cn	北京邮电大学
s1b.time.edu.cn	清华大学
s1c.time.edu.cn	北京大学
s1e.time.edu.cn	清华大学

3.5 用户管理

3.5.1 概述

80%的安全问题是由用户产生的，90%的日常维护工作发生在用户端。

对用户的认证、授权和记账（Authentication、Arthorization、Accounting, AAA）是典型的技术层面上的管理内容。但对用户的管理所包含的内容远不止于此，手段也不仅仅限于技术。因此，对用户的管理是网络系统规划、实施的难点，涉及各个层面，是网络系统运行维护工作的重点内容之一。

本节重点讨论对用户管理的技术方案的规划办法，有关组织、行政等方面的管理手段请参见《北京地区医院信息系统基础设施运行与管理规范》。

3.5.2 用户管理的内容

尽管用户管理所包含的内容很多，但归纳起来包括三方面的内容：用户身份管理、用户上网行为的监控与管理、用户端系统的管理。

用户管理是信息安全的重要组成部分。

3.5.3 用户身份管理

用户身份的管理首先要保证用户身份的唯一性，实现对用户身份

的认证。为此要在全院范围内建立起统一的认证中心，为实现全院范围的单点登录奠定基础。

其次是权限管理、用户角色的规划，包括普通用户的角色设置和系统管理用户的角色设置。角色设置一般可根据应用、岗位进行多轴向设置；可采用用户组进行角色定义，用户组可以嵌套，但注意嵌套层次不宜过深。

再次是认证协议。认证中心必须支持多种认证协议。如 LDAP、RADIUS 及 802.1x 等。

第四是管理方式。认证中心必须支持集中及分层管理。

第五是支持证书的分发与管理。

第六是制定较强密码策略。

3.5.4 用户上网行为的监控与管理

在用户认证的基础上对用户的上网行为进行监控与管理是保证信息安全的手段，也是有效预防安全事件、防止安全事故的有效措施。

用户上网行为的监控与管理主要集中在以下两个方面：

1．院内资源访问行为，如监控软件和硬件的非法安装、私自变更上网参数，如 IP/MAC 地址等。

2．Internet 访问行为。如网络资源的滥用和访问非法网站等。

《中华人民共和国互联网安全保护技术措施规定》（公安部令第 82 号）中规定，用户的所有 Internet 访问行为均要有日志。

3.5.5 用户端系统的管理

对用户端系统的管理包括以下三方面的内容：

1．设备硬件及操作系统的维护与管理；

2．应用系统软件的维护管理；

3．接入网的控制。

前两项请参考《北京地区医院信息系统基础设施运行与管理规范》。接入网的控制是指用户端设备必须满足一定条件，例如，只有安装了所规定的防病毒软件和最新的补丁，才能获得 IP 地址及其他配置参数。

为方便对用户端系统的管理，应做到：统一硬件配置，统一软件安装，统一命名规范，统一集中管理。

3.6 补丁管理

补丁管理包括：

1．评估

评估需要打补丁的环节，医院环境通常要注意：硬件设备，如交换机、服务器的内置操作系统；服务器、桌面系统的操作系统；桌面系统的实用工具软件，如，微软的 Office；应用软件系统。

2．识别

及时发现新补丁，及时发现未打补丁的环节。

3．规划

新补丁的发布应该符合生产环节中正确的变更流程，确保该变更不会危及关键业务。

4．实施

服务器应采用手工实施补丁，普通桌面终端应借助桌面管理软件。

3.7 病毒防范

病毒防范的关键在于根据医院的网络情况、业务特点和支持能力，制定出合理的防病毒策略和防病毒的体系结构。

有效的防病毒体系结构包含的基本内容是：

1．建立集中管理与分级管理相结合的病毒防护管理体系；

2．建立防病毒的响应体系，必要时纳入防病毒厂商；

3．培训，提高防毒意识和病毒排查能力。

有效的防病毒策略应包含如下内容：

1．集中安装、统一策略管理和分组管理；

2．集中定期检查和远程控制；

3．定时升级，保证病毒防护系统的实时更新；

4．病毒事件报警、应急响应、日志分析和疫情通报；

5．移动客户端的管理。

4 网络系统建设

4.1 概述

网络建设应按照项目管理的方式进行，通常划分为准备阶段、实施阶段、系统切换阶段、试运行阶段和验收阶段。

4.2 准备阶段

准备阶段的工作包括：

1．网络系统的现状调查，进而整理出施工方案；

2．网络基础知识培训和产品技术培训；

3．技术实验。

准备阶段工作越细致，实施方案就越准确，实施成功率也越高。

4.2.1 现状调查

网络建设阶段的现状调查与规划设计阶段的现状调查有所不同，前者的重点是分析应用需求和明确目标，目的在于网络功能的设计；后者的重点在于网络系统的细节，如设备型号和配置、光纤端口类型、不同科室可以进行施工的具体时段等，目的是整理分析出具体施工所需要的各方面、各层次的详细信息，是制定施工计划及文档的前提。

调查分为物理链路、逻辑设置和施工环境三方面内容。

1．物理链路

1）机房（设备间）的位置与彼此间的距离

2）机柜所在的位置与使用情况

3）所有光缆的起止位置及链接使用情况

4）现有网络设备位置以及与配线架的链接情况

2．逻辑设置

1）VLAN 的详细设置信息与分布情况

2）设备端口的 VLAN 设置情况

3）IP 地址分配情况

4）现有应用的分布和特殊端口的使用情况

5）子网（VLAN）间访问控制的详细设置

6）互联 IP 的详细信息

7）静态路由的设置信息

8）用户控制与管理状况

9）DHCP 的使用与配置情况

10）名字服务的使用情况

11）时间服务的设置情况

3．施工环境

1）相关科室和应用可以进行施工的时间段

2）各相关部门负责人及联系方式

将收集到的数据进行整理、统计分析，得出网络施工文档。

4.2.2 网络技术培训

培训内容包括：网络知识培训、产品技术培训。

培训的对象是：项目参与人员和系统维护人员。

4.2.3 技术实验

技术实验的目的是结合实际的网络拓扑，验证网络中关键技术的可行性，确定实现方法及配置步骤。

技术实验的输出文档有实验报告和设备配置手册等。其中实验报告是学习经验的总结，也是项目归档的重要文档。

实验中的一项重要工作是统一同一类设备的软件版本。

4.3 实施阶段

实施阶段的主要内容包括：细化网络系统的实施内容、完成网络系统的联调、设备安装。

4.3.1 实施方案的细化

细化的实施方案能够用以配置每个参数，输出文档包括每台设备的物理配置和逻辑设置内容，如：设备所配置的模块类型、端口和 IP 地址、VLAN、路由等详细互联参数。

4.3.2 系统联调

系统联调包括设备联调和管理系统联调两部分内容。联调遵循自上而下的原则。主要步骤包括：核心层设备联调，核心层＋汇聚层设备联调，接入层设备联调，服务器群接入联调，对外互联的联调，网络管理系统联调。

4.3.3 设备安装

设备的安装也应自上而下进行，顺序为：

1. 核心层设备
2. 汇聚层设备
3. 接入层设备

在安装过程中的每一步都应使用网络管理系统验证安装的结果。

4.3.4 网络测试

此测试是在没有接入用户、不加载业务的情况下进行的，是为了验证设备的正确安装和正确链接。是基本重复网络系统联调阶段的连通性测试和冗余性测试（包括链路、模块、路由三个方面的冗余性）。

4.4 切换

切换阶段是把医院的应用系统和用户从老网络中切换到新网络中。这一阶段涉及到信息系统的多个层面，工作的难度最大。

制定切换方案要综合考虑应用系统运行特点和分布情况、用户的使用特点和分布情况、原网络的核心设备配置情况、网络基本服务配置情况、切换的人力物力资源情况。要区分关键业务和非关键业务、关键用户和非关键用户，并把关键应用和关键用户受到的影响降到最小。

系统切换方案的要点：

1．制定新、老网络互联的方案；

2．细化切换内容；

3．确定切换方法；

4．服务器切换方案；

5．切换时间的选择和分配；

6．切换失败的恢复措施；

7．实施方案的告知。

4.5 试运行阶段

试运行阶段的主要任务是：跟踪、监控、分析网络系统的运行和使用情况，验证新建网络的各项功能指标是否达到设计要求，对发现的设计缺陷和实施错误进行改正，为将来的维护提供优化建议。

4.5.1 试运行阶段的工作

此阶段有两项工作，一是观察应用系统运行情况和用户的使用情况；二是使用网络管理系统分析网络的运行情况和可能存在的问题。

工作内容如下：

1．统计用户的使用情况

统计故障并进行分类，以此整理出故障排除的流程和措施。建议通过建立知识库形成优化的故障处理流程。

2．监控网络设备的运行情况

统计网络中数据类型和相应流量，分析网络设备的 CPU 利用率和内存利用率，分析网络主干的带宽利用率和传输速率，分析网络高峰时段的网络承载能力，分析设备日志。从数据中判断问题。建议以周为时间粒度，输出报表。

3．监控网络路由表的变化情况

查看路由表内容是否完整，通过路由跟踪确定是否与设计方案相一致。

4．监控网络服务器的运行情况

监控主要服务器在运行高峰时段的 CPU、内存和磁盘的利用率，观察、测量用户端的访问速率，以确定网络的时延是否在设计范围内。

5．网络系统交接

此过程也可以放在系统验收之后。包括相关文档的交接和系统维护的交接。

4.5.2 网络系统优化

对试运行阶段出现的一些问题进行纠错性维护和完善性维护。

在试运行阶段结束后要出具报告表明网络系统可以正式运行。内容如下：

1．通过量化的数据或报表说明网络的性能和运行情况；

2．相关问题的解决；

3．提出系统维护的建议方案；

4．总结试运行阶段的情况，建议系统正式投入运行。

4.5.3 制定网络运维流程

在网络系统正式投入运行的同时，医院必须建立起符合自己实际情况的网络系统维护流程和操作规程。

运行维护可划分为日常运行维护和应急运行维护两部分，日常运行维护占据医院信息中心大量的人力物力资源，建议采取建立知识库、故障分类、优化故障处理流程等方法提高效益、减少工作量。应急运行维护要有应急预案。

制定网络运行维护流程首先要确定维护内容和范围；其次是对内容进行分类，明确岗位和职责，确定工作流程；最后选派人员上岗。

运行维护流程要根据情况的变化作相应的调整。详细情况请参见《北京地区医院信息系统基础设施运行与管理规范》。

4.6 验收阶段

验收阶段主要的内容包括：制定验收方案，整理归纳文档，制定管理制度，召开项目验收会议。

4.6.1 制定验收方案

验收前要做如下准备：成立验收小组、确定验收程序、准备验收资料。

通常验收资料包括以下内容：

1．整理项目文档。包括：设计文档、配置文档、维护文档、设备随机资料、项目的管理文档等。

2．交接审查。集成商要提供一份双方签字的合同设备交接单，注明设备型号、数量、状态以及设备的分布表。

3．制定测试方案。项目验收前应制定网络测试方案。测试方案是根据设计方案制定的对新网络整体性能进行测试的内容和方法，区别于实施过程中的层面测试。测试方案是网络测试的依据及指南。

4．网络测试。根据网络测试方案对网络进行测试并形成测试报告。测试报告是项目验收的必备资料，医院领导和专家通过它可以定性和定量地了解网络系统的基本情况。

5．编写工程技术报告。项目的工程技术报告主要说明项目的背景、项目要解决的问题和采用的主要技术手段。

6．编写工程实施报告。项目的工程实施报告主要是说明项目的实施依据、实施目标、实施步骤、实施结果、结果偏差对比和项目实施结论。

4.6.2 整理文档

在项目的众多文档中，技术文档包括网络系统配置资料和网络系统维护资料，是最重要的文档，详细记录了系统的配置内容和运行维护的流程及方式。在归档时，应该包括前期的设计文档。

技术文档的整理不仅是对系统实施过程中产生的文档汇总，而且是根据网络系统维护的需要对已经有的技术文档进行重新梳理，还是技术和经验的总结。技术文档需要根据系统的变化而调整。

一般来说，网络系统的配置资料包括以下内容：

1．网络拓扑图及相关信息

包括主干拓扑图、以汇聚节点为单位的接入拓扑图和网络出口的链接图三种，拓扑图中要充分体现互联的信息。

1）主干拓扑图中包含的信息

（1）设备名称

（2）设备管理地址

（3）互联端口及端口类型

（4）互联地址及掩码

（5）有的可能含 VLAN_ID 及 VLAN_NAME

2）以汇聚节点为单位的拓扑图中包含的信息

（1）设备名称

（2）设备管理地址

（3）互联端口及端口类型

（4）互联地址及掩码

（5）VLAN 信息，如：VLAN_ID、VLAN_NAME、VLAN 的网关及所属设备端口等

（6）汇聚层与接入层设备互联的 Trunk Port

3）网络出口的链接图中包含的信息

（1）设备名称

（2）设备管理地址

（3）互联端口及端口类型

（4）互联地址及掩码

（5）路由策略

（6）安全策略

2．网络 IP 地址分配表

网络 IP 地址分配包括网络管理地址、网络互联地址、服务器使用和用户使用等。

3．网络设备配置手册

在医院网络的架构中，包含三种层次的网络设备：核心层设备、

汇聚层设备和接入层设备。设备配置手册是网络维护的必备资料，它的编写是以网络设备的《配置指南》为蓝本，按照实际配置内容的需求，结合设备的类型和配置模块，定制所需要的命令、格式、内容和步骤。网络设备配置手册也分为核心层、汇聚层和接入层。

4．网管配置手册

网管配置手册也是网络维护的必备资料，它的编写是以网管系统的《用户手册》为蓝本，按照实际配置内容的需求，详细记录网管系统的安装、配置等步骤。把配置过程中图形界面放入文档中，能够更易于理解和使用。

5．服务器文档

记录服务器有关网络的详细信息。

6．其他设备或软件配置手册

如防火墙的配置手册、网络策略管理软件的配置手册，也是重要的维护文档。

7．布线信息点维护表

布线信息包括光纤和双绞线两部分内容。

1）光纤布线分布情况

（1）光纤链路敷设路由图及标识

（2）光纤链路测试数据

（3）光纤芯数使用情况、链接设备及端口的对照关系

2）双绞线布线分布情况

（1）双绞线链路敷设路由图及标识

（2）双绞线链路测试数据

以双绞线配线架为单位，记录缆线链接房间号、链接的设备端口及所属 VLAN 等信息。这张表结合用户 IP 地址分配表，用于终端信息的维护。

8．标签说明文档

标签说明文档用于说明标签规则，记录标签内容（参见6.6 标识系统）。

9．设备随机资料的整理

按设备类型整理归档。

10．项目管理文档

11．附件

工程实施过程中产生的一些文档，如会议纪要、工程协调单等。

4.6.3 召开验收会议

验收的准备工作全部就绪后，按照项目的验收仪式程序，召开验收会议。目的：一是倾听用户和专家的建议，作为改进的依据；二是为了得到用户和专家对项目实施的肯定。

验收会议结束后，标志着项目实施的结束和系统维护的开始。

5 网络安全管理

5.1 概述

网络安全管理的目的是通过技术手段发现并解决网络系统及其运行环境中的安全隐患，保证网络系统的运行。

网络安全管理是网络运行阶段的重要任务，但在建设阶段就应明确管理内容和手段，从而为今后实施管理创造条件。

通常网络安全管理包括对网络的监控和对安全事件的审计。

5.2 网络监控

监控的目的是了解网络真实的状态、系统应用情况和用户行为，及时发现网络系统中的薄弱点及受攻击情况。

5.2.1 网络流量流向分析

对网络设备进行流量信息采集。分析全网数据的流量及流向，检测流量类型，提供字节数、当前带宽、峰值、新增链接数、最大并发链接数、当前并发链接数等参数，并提供指定地址段之间的流量统计分析，为网络的运维提供量化的基础数据。

5.2.2 运行状态分析

运行状态分析包括：

1．网络设备运行状态分析。包括 CPU、内存利用率和连续运行时间，端口的流量及峰值等。

2．服务器运行状态分析。包括日志、安装的程序、CPU、内存、进程、磁盘分区信息管理等。

5.2.3 入侵监测/入侵防护

入侵监测/入侵防护（IDS/IPS）是安全管理的重要手段，是整个安全防御体系的重要组成部分。

IDS/IPS 可以根据网络拓扑结构和运行的业务特点来部署。

5.2.4 网络运行趋势分析

通过监控，采集、统计网络流量流向、设备运行状态以及用户行为等基础数据，以量化的指标直观地呈现各种性能数据，科学地预测未来一段时间内的网络运行趋势，做到防患未然。

5.3 网络安全审计

5.3.1 概述

安全审计是根据医院制定的安全策略对网络系统进行的安全符合性检查。通过对网络系统的历史事件及数据进行分析，发现网络系统存在的安全隐患及影响其性能的因素。目的是保护网络系统资源及责任认定。

审计的对象是网络中的主机、服务器、网络设备、网络访问行为以及它们之间的关联信息。

网络安全审计的作用是：

1. 对潜在的攻击者起到震慑或警告作用；

2. 对于已经发生的系统破坏行为提供有效的追纠证据；

3. 及时发现系统入侵行为或潜在的系统漏洞；

4. 发现系统性能上的不足或需要改进与加强的地方。

日志审计和账号审计是惯常的做法。

5.3.2 日志审计

日志审计通过代理或者 SYSLOG、SNMP TRAP 协议采集服务器主机、应用系统、数据库、网络设备和安全设备等的日志，进行分类、归并、过滤等处理，再进行格式化和统一的存储，并提供日志的查询和分析报表功能，从中获取有价值的日志信息。

日志记录的内容包括：开始时间、结束时间、协议类型、源 IP 地址、目的 IP 地址、服务类型、源端口、目的端口、报文数、字节数、流数、总激活时间、操作字、日志类型等信息。

日志审计的目的是深入了解网络中的报文所包含的各种有价值的信息，可以实现网络监控、应用监控、用户监控等功能，并为网络规划提供重要参考。

5.3.3 账户审计

账户审计是对正在使用网络资源的用户进行计费。虽然记账服务对目前的大多数医院来说不曾用到，但通过计费管理可以查询用户操作日志，以便进行安全监控管理。

这主要涉及两方面的原因：

1．法令的要求

中华人民共和国公安部令 82 号中规定互联网使用单位应落实“记录并留存用户登录和退出时间、主叫号码、账号、互联地址或域名、系统维护日志的技术措施”。记录这些数据是记账系统的基本功能，因此，实现完整的记账系统，一般就能满足这一法令的要求。

2．业务发展的需要

对用户提供网络服务（如 Internet 接入、网络探视等）需要账户管理系统。

6 网络布线系统

6.1 概述

布线系统包括七个部分：工作区、配线子系统、干线子系统、建筑群子系统、设备间、进线间、管理。

医院在网络布线建设中应遵循的标准有：

1.《国际布线标准》（ISO/IEC 11801）；

2.《建筑与建筑群综合布线系统工程验收规范》（GB/T 50312-2007），《建筑设计标准》（GB/T 50314-2000）；

3.《智能建筑设计标准》（GB/T 50314-2000）；

4.《中华人民共和国通信行业标准》（YD/T 926.1-2001）；

5.《工业企业通信设计规范》（GBJ 42-81）；

6.《民用建筑电气设计规范》（JGJ/T 16-92）。

6.2 规划原则

1．标准化原则

布线系统的必须遵从布线系统的相关标准以及产品厂商的技术操作要求。

2．需求驱动原则

布线系统的规划设计是在网络拓扑的设计方案基础上进行的，网络布线系统的规划设计方案必须满足网络拓扑的互联要求。

3．统一规划原则

布线系统的实施可以分步，但规划最好全局考虑，应做到：统一规划不同应用（语音、视频、监控），统一规划内、外网，统一规划不同地理区域，统一规划材料的规格指标。

4．灵活性原则

布线系统要考虑多方面的需求，使系统组网灵活多样，各部门可独立组网、方便互联。设备间的彼此互联要尽量多。

5．可扩展性原则

要充分考虑各种设施的扩充余量，包括机房面积、机柜容积、线槽容量等。

6．可维护性原则

在网络布线和设备安装过程中应考虑维护的可行性。设备间数量要尽量少、缆线尽量集中，从而减少设备间的数量。不同用途的缆线应放置在设备间或机柜的不同位置，以减少相互地干扰和人为的差错。

6.3 规划设计的内容

布线系统的规划设计内容主要涉及以下工作：现场调研，设备间，各种线缆数量（容量），各种线缆的路由，线缆及设备的标识规则，各种设备的指标、型号。

6.3.1 现场调研

此阶段调研的目的是进一步探明施工现场的环境，确认信息点的位置、数量以及线缆的路由，是网络布线深化设计的重要依据。

首先确定调研方案，主要考虑以下多方面的因素：

1．确认网络规划对布线系统的要求；

2．探明楼宇分布和管道竖井的位置，计算出弱电管道竖井与设备间的距离；

3．了解建筑的结构、装修特点及对施工方案的限制，确定线缆的路由，选用合适的线管、线槽；

4．确认设备间的位置、面积及运行环境的要求（周边有无电磁

干扰）；

5. 掌握医院未来发展规模，确认各部门信息点数量。

6.3.2 设备间的确定

除了 90m 的距离限制外，设备间位置的选择要考虑以下问题：

1．满足设备间的制冷、保温、防水、防雷、防尘等要求；

2．有 UPS 系统时应考虑承重要求；

3．易于管理，尽量减少设备间的数量；

4．消防要求；

5．设备运输要求。

6.3.3 容量的确定

6.3.3.1 信息点数量的确定

1．信息点的数量一般遵循偶数原则。

2．根据房间功能确定。建议在所有办公区域内均布设网络，即每个单独工作室最少 2 个信息点。

3．根据房间使用情况确定信息点数量。

4．开放式办公区域信息点数量确定。大会议室、公共场所（如大办公区、病房移动 PDA 等应用）应该考虑无线覆盖，按无线设备的覆盖区域范围，合理安排无线信息点数量。

5．备份链路对信息点数量的影响。对门诊挂号、收费等重要区域的用户，一般应考虑备份链路，因此信息点的数量和位置应有特殊考虑。

信息点具体数量见下表：

区域或用途	敷设数量	是否设置 AP
办公区域	2 点/工位 或 2 点个/6~8 m^2	是
会议室	至少 4 点	是
病区医生办公室	1 点/5 张床	是
病区护士站	4 点	是
ICU	2 点/床	是
门诊诊室	2 点/诊桌	
门诊分诊台	4 点/个	
门诊窗口	2 点/个	是
手术室	6 点/间	是
窥镜科室	2 点/窥镜	是
大型影像设备	4 点/台	
影像读片室	1 点/3 m^2	
检验科	2 点/设备	
超声检查室	2 点/设备	

6.3.3.2 主干光纤的数量

网络规划所需铺设的光纤应不少于 16 芯。

建议在同级设备间之间敷设横向互连光纤，以增加网络的可扩展性并做物理链路的冗余。

6.3.3.3 无线 AP 的确定

无线 AP 的数量和位置通常根据应用需要和建筑物格局来确定。在规划 AP 时要注意不同产品的覆盖能力存在差异，数量也不同。

6.3.4 缆线路由的确定

影响缆线路由的因素很多，除考虑建筑物的格局外，应特别注意有强电、强磁存在的区域，如放射科等部门。

6.3.5 线缆的选择

6.3.5.1 光缆的选择

光缆通常用于网络布线的主干链路中。

距离小于 300m 时采用多模光纤，大于 300m 选用单模光纤。

选择光缆时，应依据现场的安装环境合理确定光缆的类别。

6.3.5.2 双绞线的选择

医院布线系统中的双绞线通常用于水平布线。一般可选用非屏蔽超五类双绞线。对放射科、手术室等存在电磁辐射干扰的特殊区域，建议采用全屏蔽系统或光纤系统。

对高带宽要求部门，可采用六类线缆布线。

6.4 深化设计

在现场调研的基础上对前期的布线规划设计进行深化，整理出用于实施的深化设计。深化内容应包括：

1．确定工作区信息点位置

信息点位置应尽量靠近计算机和电源插座。

2．配线子系统

1）进一步确定网络布线系统各科室水平区采用的传输介质。

2）确定楼宇设备间的位置后，计算出水平信息点线缆长度，并根据信息点平均缆线长度和信息点数量计算出全部信息点所需线缆需求数量。任何一个信息点的缆线长度不应超出 85m。

3）计算配线架数量，一般采用 24 个端口和 48 个端口两种规格的配线架，信息点数/24（48）=配线架数量。

4）根据信息点总数，计算出机柜数量，配线架机柜应采用 19 英

寸标准机柜。建议首选 2m 机柜，一个 2m 机柜一般最多链接 240 个信息点。

3．主干子系统

1）计算主干光缆长度，根据设备间之间路由距离计算光缆长度，计算光缆长度时要考虑光缆两端至少各留有 10m 的余量。

2）确定室内或室外光缆的类别。一般楼宇内采用室内多模光缆，楼宇之间采用室外光缆，同时还应考虑防雷问题，建议选择轻铠光缆。

4．管理区

为了保证设备正常运行，管理子系统必须：

1）依据设备间信息点数量确定管理区配线架的容量；

2）制作管理区的安装示意图或表格；

3）标识配线架管理区，区分各配线架对应的区域。

5．确定辅助材料

1）桥架规格和长度：根据线缆总数和路由总长度、计算所需各种桥架（线槽）规格和长度。考虑医院特殊环境，桥架（线槽）应采用防火材质，建议采用镀锌桥架，缆线在桥架中的充填度不大于桥架横截面积的 60%。

2）线管规格及长度：楼道桥架到房间内插座盒之间必须使用线管，采用明装时应使用镀锌钢管，砌入墙内的暗装线管选用镀锌钢管或 PVC 塑料材料，内径应大于 20mm。

6．编制工程预算

整体方案确定后，根据最后方案修正的材料规格、数量和价格，并按《北京市建设工程预算定额》编制工程正式预算金额。

6.5 建设过程

6.5.1 施工准备

施工准备是网络布线工程的必要步骤，是保证施工质量和工期的重要环节。

6.5.1.1 准备施工文档

施工文档主要包括：施工路由图、信息插座分布图、配线架表、光纤表和机柜分布图等。

施工路由图是在楼宇图纸上标明桥架和线管的位置走向。

信息插座分布图纸是在楼宇图纸上标明信息插座位置及其编号。

配线架表内容包括：楼宇名称、楼层、房间号、信息插座号、配线架号、交换机名称、交换机端口号、备注等字段。一般每个配线架一张表。

光纤表内容包括：光纤类型、起止端设备间楼号、设备间号、主设备间机柜号、光纤配线架号、光纤配线架端口号。

机柜布置图：记录机柜中配线架数量及位置。

6.5.1.2 编制详细的施工组织方案

方案主要包括：项目总体目标计划、工程项目资源分配、项目进度计划、项目质量安全计划、施工工序、工艺方法及技术措施计划等。

6.5.1.3 制定施工计划

按照器材准备、施工量、人数、施工环境、施工难度等因素，制定详细的施工计划。包括：材料到货计划、人力资源计划、施工机具使用计划、施工进度计划等。

施工进度计划必须依据医院各科室具体工作性质和不同的作息时间，分别制定合理的施工进度计划，尽量避免干扰业务。

6.5.1.4 其他

安全文明施工的宣贯。

检查相关的施工用具，安全警示设施等。

6.5.2 施工阶段

该阶段包括路由施工、水平缆线铺设、垂直缆线铺设、对线、终接、线缆标识、测试、验收、布线系统标识等步骤。施工必须遵照GB 50311-2007 标准和 GB 50312-2007 标准要求。

由于布线系统的施工一般均由布线专业公司完成，对施工过程不再介绍。

6.5.2.1 线缆标识

在施工过程中对线缆进行的标记往往与最后的线缆标签是不同的，施工时的线缆标记既是为方便施工所做，也是为将来进行线缆维护提供便利，因此也要纳入标识系统一同考虑。

对线缆标识请参照“6.6标识系统”一节。

6.5.2.2 对线

在线缆敷设完成后、线缆终接之前，需要进行对线。对线过程是借助仪器检测出每条缆线对应的信息插座位置，在线缆上标识。目的是确认楼层设备间内每条缆线的来源，保证配线架上端口号顺序，与信息点在物理空间位置相符合。

在对线时，应该注意以下几点：

1．标识包括楼号、楼层号、房间号、信息端口号；

2．在做标识前需要确定缆线的保留长度，缆线保留长度=设备间内预留长度 0.5~1.0m＋机柜高度＋终接长度 1.0m；

3．标识位置距离保留长度端点至少 1.0m。

6.5.2.3 测试

1. 综合布线系统测试，采用 ANSI/TIA/EIA 568B 综合布线测试标准。主要有以下几种类型：超五类系统测试，六类系统测试，光缆测试（分单模、多模测试）。

2. 测试仪器

应使用符合相关标准的合格测试仪器。

3. 测试方案

主干电缆 100%实地测试，水平电缆 100%实地测试。

测试报告：对于测试发现不合格线缆，必须根据不合格参数查找原因进行改正。

6.5.2.4 验收

综合布线完成后，应形成验收报告。竣工文档包括：竣工图纸，各管理区设备配置图，各管理区设备配置表，维修保证书，性能保证书，综合布线系统管理参考手册，测试报告，应急联系人，联系方式等。

6.6 标识系统

标识是对管理对象进行命名、标记的过程。标识的目的是指导系统维护人员在工作现场能方便地识别出其操作对象的位置、状态以及与周围环境的关系，同时有利于文档的书写、说明。

按照 TIA/EIA-606 标准，布线系统的五个部分需要标识：线缆（电信介质）、通道（走线槽/管）、空间（设备间）、端接硬件（电信介质终端）和接地。但标识系统部不应仅限于这五个部分，应该对更大范围的管理对象进行统一标识，为今后的运行维护工作创造条件。

在制定标识规则时要考虑到今后使用软件进行管理的需求。

6.6.1 标识系统的内容

在制定标识系统时，应考虑的管理对象包括：楼宇的标识、房间的标识、机房（设备间）的标识、机柜的标识、配线架的标识、线缆的标识、设备的标识和服务器的标识。

6.6.2 标签的位置与内容

标签要放置在醒目的位置，必要时可在多个方位放置标签。标签上的字号要尽可能大一些，要尽量选择笔画粗的字体、颜色要明亮。

下表是主要管理对象的标识内容：

	管理对象	标识内容	标识位置
1	楼宇的标识	原有名称	-
2	房间的标识	原有编号	-
3	机房（设备间）的标识	原有编号	-
4	机柜的标识	机柜编号	机柜前后
5	配线架的标识	机柜编号	配线架面板
6	线缆的标识	线缆标号	两端及面板
7	链接线（跳线）	两端所连对象	两端
8	设备的标识	设备名称 管理 IP 地址 电源插口	设备前后[注] 插口旁
9	服务器的标识	设备名称 网卡编号 IP 地址 电源插口	设备前后 网卡插口旁 设备前后 插口旁
10	信息点插座	线缆标号	面板
11	电源插座	插座编号	面板
12	插销板	插销板编号 插孔编号	面板 插孔旁
13	设备电源线	两端所连对象	两端

注：设备的标识除了在设备外表贴标签外，还应做内部标识。

6.6.3 标识材料和方式

粘贴型：粘贴标签应满足 UL969 中规定的清晰、耐磨损和附着力的要求。

插入型：插入标签应满足 UL969 中规定的清晰、磨损性和一般外露要求。

其他：其他标签包括用不同方法粘贴的特殊用途的标签。

标识材料要耐磨、稳固、考虑两端、耐腐蚀，并且防水。标识除了清晰、简洁、易懂外，还要尽量美观。

6.7 电子配线架

随着医院信息系统的迅猛发展，在信息管理人才不足的情况下，可以考虑使用较为先进的电子配线架，以提高管理效率。其主要功能体现在：

1．支持使用标准铜缆跳线链接；

2．自动端口发现功能；

3．断路报警功能；

4．单键追踪功能；

5．CAD 图形格式支持；

6．工作任务报警；

7．支持使用标准光纤跳线链接；

8．每个机架单元配置大型 LED 显示, 可使维护人员进行电子查询。

7 机房建设及相关标准

7.1 概述

中心机房和设备间（以下统称机房）是放置各种硬件设备的场所，特别是中心机房存有关键设备，其内部设施和环境的安全直接影响到设备的稳定运行和寿命，而且维护点较多，需要给予特殊、充分的重视。

医院目前主要存在三大类机房：中心机房、设备间、其他设备间。

大型医院还有可能将中心机房分为：数据中心、网络中心和管理（运行）中心，但在建设规格上还应按照这三类机房来设计。

针对不同的机房，基本要求也有高低之分：中心机房主要用于数据存储、网络运行和运维管理，要严格遵从相关标准进行设计规划；设备间主要用于存放网络设备，最好遵从相关标准，但可根据设备情况灵活掌握；其他机房要按照各自功能分别进行设计规划，但 UPS、空调、防雷、空气净化、接地等是必须的配套设施。

机房设计建设应遵循的标准有：

1. 《电子计算机场地通用规范》（GB 2887-2000）
2. 《电子计算机机房设计规范》（GB 50174-93）
3. 《电子计算机机房施工及验收规范》（SJ/T 30003-93）
4. 《计算站场地安全要求》（GB 9361-88）
5. 《计算机机房活动地板技术条件》（GB 6650-86）
6. 《智能建筑建筑设计标准》（GB/T 50314-2000）
7. 《供配电设计规范》（GB 50052-95）
8. 《建筑物防雷设计规范》（GB 50057-94）
9. 《建筑物电子信息系统防雷技术规范》（GB 50343-2004）
10. 《火灾自动报警系统设计规范》（GB 50116-98）

7.2 机房设计原则

机房设计的原则可考虑如下几个方面：

1. 标准化原则

结合医院的系统状况及发展规划，遵循国家相关规范和标准，设计满足医院使用需求且符合标准的机房方案。

2. 前瞻性原则

机房设计要结合系统运行特点和现有系统及预期发展的因素，采用先进的技术措施，编制出技术先进、经济合理的设计方案。

3. 扩展性原则

机房的设计应具备扩展性，能满足医院的长远发展，最好具有 10 年的生命周期。

4. 适应性原则

机房设计与网络规划、布线规划应相互关联，整体一致。机房内的场地空间可根据系统运行需要进行必要的灵活性调整。

5. 可管理性原则

要充分考虑机房的可管理性、易维护性。

7.3 机房规划、建设内容

7.3.1 中心机房选址

中心机房的选址应按照相关国家标准综合考虑，并结合医院需求及实际情况综合考虑。同时注意以下因素：

1．机房所在楼层的上下层避免是厕所、澡堂、水房、化学实验室等；

2．机房一定要远离电磁场干扰；

3．机房要求有专用的供电，而且应有双路供电保证；

4．机房要求有运输及消防通道。

7.3.2 中心机房的组成

中心机房按功能区可划分为第一主机房、第二主机房、电池室、基本工作区、维修室、资料室、备件库等。另外，根据需求可设置会议室、值班室、生活间、洗手间等。

7.3.3 中心机房的面积

中心机房的位置一旦确定，就很难移动，因此，中心机房的建设要有长远计划。中心机房的大小直接影响其寿命和可扩展性。

1．按照职工数量计算中心机房的面积

职工数	机房面积
<100	1.0m^2/职工
200~250	0.5m^2/职工
400~500	0.4m^2/职工
1500~6000	0.2m^2/职工

2．按照设备数量计算主机房（包括第一主机房和第二主机房，下同）的面积

服务器和其它设备数量不仅包括当前设备的数量，而且应考虑未来十年所需。

建议设备尽量选择机柜式设备。塔式设备参照机柜计算。

主机房的使用面积应根据计算机设备的外形尺寸布置确定，使用面积应符合下列规定。

计算公式：$A=K\Sigma S$

式中：A—计算机主机房使用面积（m^2），最少不得低于 50 m^2；

K—系数，取值为 8~10[5~7（含有未来扩展的系数）]；

S—计算机系统及辅助设备的投影面积（m^2）。

下表是某三级医院信息中心机房建设中各功能区面积配置清单，供各医院参考使用。

序号	名称	面积 (m^2)	备注
1	主机房	60	按公式换算,规模小的医院可以略小
2	UPS 配电间（含 2 小时电池组）	19.6	
3	软件、硬件办公区	60	按 4.0m^2/人，15 人计算，不含开发人员办公区
4	维修间	20	依据各医院具体情况配置
5	新风室	5	依据各医院具体情况配置
6	网管间	12	依据各医院具体情况配置
7	备件间	9	依据各医院具体情况配置
8	更衣换鞋间	6	依据各医院具体情况配置
9	夜间值班室	10	依据各医院具体情况配置

10	缓冲间	3	
11	小计	204.6	

说明：消防系统如果是无管网则安装于主机房内，如采用管网则安装于 UPS 间或单独配置一间设备间。

3．经验值

一般三级以上医院的主服务器机房面积配置在 75~100m^2较为适宜，不能少于 60 m^2；二级或以上的医院至少应大于 50 m^2。

7.3.4 其他机房面积

其他机房包括：汇聚设备机房、一般设备间、UPS 机房、电池室等。

设备间面积：一般设备机房的面积一般大于 8 m^2。

电池室面积：电池室面积一般大于 10 m^2。

7.3.5 空气调节

7.3.5.1 机房空调环境要求

医院机房空气环境设计参数（根据《电子计算机机房设计规范》（GB 50174-93）和《计算站场地技术要求》（GB 2887-89）中规定机房的温湿度要求）：

夏季温度	23±2℃	冬季温度	20±2℃
夏季湿度	55±10%	冬季湿度	55±10%
洁净度	粒度≥0.5μm	个数≤18000 粒/分米^3	
温度变化率	≤5℃/时		

主机房的洁净度则要求做到以下几点：

1．机房要密封，墙体围护结构要清洁；

2．机房要保持正压，防止脏空气侵蚀。新风做到两级净化，即初效、亚高效过滤器，从而使输入机房空气洁净度大大提高；

3．空调机设中效过滤器，并定期更换，从而保证机房空气在不断循环中得以净化。

7.3.5.2 机房空调的容量选择

空调制冷量的选择：

1．依据《电子计算机机房设计规范》（GB 50174-93），空调制冷设备的制冷能力应留有 15%~20%的余量；当计算机系统需长期连续运行时，空调系统应有备用装置。

2．医院信息中心机房内设备集中，密度大，热负荷也较其他行业大（电信、金融行业除外）。依据实践经验，建议采用 350Kcal/m^2.h 计算较为合适。

3．尽量配置两台，增加机房空调的可靠性。

7.3.5.3 选择机房空调送风方式

机房空调送风方式分为：上送风方式、下送风方式、弥漫式。

送风方式可依据机房的结构进行选择。在机房抗静电地板有一定的净高度（大于 350mm,最好在 500mm 高度），且地板下没有明显的阻风设施，建议采用下送风的空调系统；反之，则采用上送风的空调系统；弥漫式的空调系统一般适用于机房面积较小的楼层设备间或汇聚层设备间里安装。

7.3.6 医院机房供电系统

7.3.6.1 配电设计内容

主机房供电系统主要包括：主机房设备 UPS 用电、UPS 本身用电、照明用电、消防用电、安防门禁用电及其他辅助区域用电。

依据主机房用电量（即 UPS 视在功率）和相关辅助设备用电量，确定信息中心实际用电负荷；再考虑未来 5 年机房用电扩展负荷量，计算出总的用电负荷（一般：20KVA、40KVA、60KVA、80KVA、120KVA、160KVA）。由医院供电部门负责敷设独立的供电回路（医院配电室—信息中心配电箱）。此回路在医院配电室端应有双路供电保障。总进线电缆采用三相五线制或单相三线制。

7.3.6.2 电源质量要求

第一主机房供电系统应符合《电子计算机机房设计规范》（GB 50174-93）中“第六章 电气技术”的要求。

在《电子计算机机房设计规范》（GB 50174-93）中对电压变动、频率变化、波形失真率均有具体的分级要求（见下表）。

级别	A 级	B 级	C 级
电压波动范围	±5%	±7%	15%~+10%
频率波动范围	≤±0.2Hz	±0.5Hz	±1Hz
波形失真率	3~5%	5~8%	8~10%

在医院机房的设计中供电标准应选用 A 级标准。

主机房供配电系统应考虑计算机系统有扩展、升级等可能性，并应预留备用容量。

对供电可靠性要求较高，需要保证顺序断电安全停机，业务主要计算机系统等应采用 UPS。

单相负荷应均匀地分配在三相线路上，并应使三相负荷不平衡度小于 20%。

电源进线应按现行国家标准《建筑防雷设计规范》采取防雷措施。

UPS 应尽量考虑选择在线式，设计容量应该考虑实际负载容量小于 UPS 额定容量的 60%。

7.3.6.3 配电箱及电源插座

1．配电箱

主机房必须设置专门的配电箱（柜），提供多路 380V 电源供电。

配电箱通常有总进线箱（柜）、普通电源配电箱、UPS 电源配电箱。总进线箱（柜）的绝缘性能应符合国家标准 GBJ232-82。普通电源配电箱、UPS 电源配电箱配置应有适合每个配电回路的空开（特别是向各设备柜供电的空开，通常选用 20A、32A 或以上的空开），应有防浪涌保护器，应按国家规定的颜色标志编号。

2．电源插座

主机房内各设备使用的插座容量要符合设备对用电量的要求，并有一定的冗余量。

主机房内插座安装的位置一般在抗静电地板下或直接接进机柜里；也可以安装在使用方便但较为安全的地方。

有足够的电源插座，每个电源插座的容量应不少于 300W 负荷。

禁止用临时的照明开关控制上述电源插座，减少偶尔断电事故发生的频率。

机柜内不宜使用插线板；必须使用时，应避免使用有开关的接线板。

7.3.7 照明

主机房按《电子计算机机房设计规范》（GB 50174-93）要求，主机房的平均照度为 300Lx；其他辅助功能间照度不小于 200Lx；机房疏散指示灯、安全出口标志灯照度大于 1Lx。

7.3.8 防雷、接地系统

7.3.8.1 机房防雷

机房建设在设计、安装防雷产品时必须遵循下列规范：

1.《建筑物防雷设计规范》（GB 50057－2000）

2.《电子计算机机房设计规范》（GB 50174-93）

3.《浪涌保护器的要求》（IEC 61312-3）

4.《建筑物电子信息系统防雷技术规范》（GB 50343-2004）

机房电源部分采取三级防护。有关雷电防护区的划分请参见《建筑物电子信息系统防雷技术规范》（GB 50343-2004） P6 页“雷电防护分区”。

机房防雷主要注意以下方面：

1．机房总进线箱；

2．UPS 电源配电箱；

3．机房内 UPS 电源插座；

4．进入机房内的各种通讯线缆应采用信号防浪涌保护器。

7.3.8.2 静电防护

机房静电防护应符合《电子计算机机房设计规范》（GB 50174-93）的相关规定。

7.3.8.3 机房接地

机房接地应符合《电子计算机机房设计规范》GB 50174-93 的相关规定。防雷保护接地 必须严格执行《建筑物电子信息系统防雷技术规范》GB 50343-2004 的相关规定。机房接地主要包括以下部分：

1．安全保护接地，即机房内所有设备外壳及空调等设备机壳接

地。

２．防静电接地，即机房设备和静电地板接地。

7.3.9 机房环境监测系统

机房环境监测系统是指对机房的电、水、温度、湿度、机房空气及机房供电异常的报警进行监测。

建议在主机房安装机房环境检测系统。检测结果应该能够在最短时间内发送给机房管理人员。

7.3.10 机房物理安全

7.3.10.1 监控系统

机房安装监控系统主要有以下需求：

1．配合医院安全部门做好安全保卫工作，实现统一监控录像存储；

2．方便机房工作人员随时监控机房工作状态，用于记录进入机房人员的工作状况；

3．监督机房管理制度的有效执行情况。

监控信号一方面传送到医院安全监控中心，另一方面送到信息中心值班室进行监控。在配置监控系统的摄像机时，应考虑夜间监控问题。

7.3.10.2 门禁系统

医院信息中心应配置门禁管理系统，主要安装于主机房、主要辅助机房、信息中心主门（有的信息中心较为分散，则无此项）。其主要作用是：

1．非信息中心人员、机房工作人员不能随意进入信息中心、机房。如需要进入时，须做好登记，并服从值班管理人员的管理。

2．自动存储出入人员的有关信息，如时间、地点等，并能有效地统计和存档记录。

3．配合信息中心管理制度的严格执行。

配置信息中心门禁时，必须严格遵守《安全防范工程技术规范》（GB 50348–2004）等国标规范。医院信息中心面积较大时，建议设置对讲系统。

7.3.11 消防安全

7.3.11.1 遵循消防规范

遵循下列有关的消防安全国家标准和北京市地方标准：

1. 《建筑设计防火规范》（GB 50222-1995）
2. 《电子计算机机房设计规范》（GB 50174-1993）
3. 《火灾自动报警系统设计规范》（GB 50116-1998）
4. 《气体灭火系统施工及验收规范》（GB 50263-1997）
5. 《消防安全疏散标志设置标准》（DBJ 01-611-2002）
6. 《火灾自动报警系统施工及验收规范》（GB 50166-1992）

7.3.11.2 气体灭火系统

主机房应设二氧化碳或卤代烷灭火系统，并应按现行有关规范的要求执行。

根据主机房面积、设备价值和工作性质，可采用移动式、半固定式或固定式二氧化碳或卤代烷灭火系统。

7.3.11.3 自动控制系统

信息中心需设置消防联动系统，应具备全自动监测、报警、联动、控制、复位等功能。

电子计算机机房应设火灾自动报警系统，并应符合现行国家标准《火灾自动报警系统设计规范》的规定。

主机房宜采用感烟探测器。当设有固定灭火系统时，应采用感烟、感温两种探测器的组合。

当主机房内设置空调设备时，应受主机房内电源切断开关的控制。机房内的电源切断开关应靠近工作人员的操作位置或主要出入口。

7.3.12 主机房的设备分布

主机房内服务器、小型机、交换机等设备尽量放在机柜内。

为了方便维护和管理，建议如下：

1．主机房内设备分布宜采用分区布置，一般可分为网络交换机机柜区域、HIS 服务器机柜区域、PACS 服务器机柜区域等不同区域；

2．机柜成排摆放时，建议不要 3 个以上机柜密集排放；

3．机柜分成两排时，建议机柜排列分出热通道和冷通道；

4．机柜后面板距离墙体（窗户）至少 1.2m；

5．机柜前面距离墙体（窗户）至少 1.8m；

6．侧面与其他机柜或墙不应小于 0.6m；

7．两个相对机柜的正面至少保留 1.8m 的距离；

8．两个相对机柜的后面至少保留 1.5m 的距离；

9．走道净宽不应小于 1.2m。

7.3.13 主机房缆线敷设

主机房内线缆主要有电源线缆和数据线缆。线缆可以敷设在活动板下桥架内或敷设在天花板吊架上。建议吊架上敷设数据线，活动板下敷设电源线。

任何架空线缆不允许直接进入主机房。

机房内的电源线应尽可能远离计算机信号线，并避免并排敷设。当不能避免时，应采取相应的屏蔽措施。

敷设的光纤、双绞线上应该标注标识，表明线缆的来源和目的。

缩写词表

AAA Authentication、Arthorization、Accounting（认证、授权和记账）

ACL Access Control List（访问控制列表）

ADSL Asymmetric Digital Subscriber Line（非对称数字用户线）

AP Access Point（无线接入点）

BOOTP Bootstrap Protocol（引导协议）

DC Domain Controller（域控制器）

DHCP Dynamic Host Configuration Protocol（动态主机配置协议）

DMZ DeMilitarized Zone（非军事区）

DNS Domain Name System（域名系统）

DoS Denial of Service（拒绝服务）

FQDN Full Qualified Domain Name（完全限定域名）

HIS Hospital Information System（医院信息系统）

IDS Intrusion Detection System（入侵检测系统）

IPS Intrusion Prevention System（入侵防御系统）

ISO 国际标准化组织（International Standards Organization）

ITIL Information Technology Infrastructure Library（信息技术基础设施库）

LDAP Light Directory Access Protocol（轻目录访问协议）

LED Light Emitting Diode（发光二极管）

MAC Media Access Control（介质访问控制）

NetBEUI NetBIOS Extended User Interface（NetBIOS 扩展用户接口）

NetBIOS Network Basic Input /Output System（网络基本输入/输出系统）

NTP Network Time Protocal（网络时间协议）

SNTP Simple Network Time Protocal（简单网络时间协议）

OSPF Open Shortest Path First（开放最短路径优先）

PACS Picture Archiving and Communication Systems（图像存储与通讯系统/医学影像系统）

PDA Personal Digital Assistant（个人数码助理）

RADIUS Remote Authentication Dial In User Service（远程拨入用户认证服务）

RIP Routing Information Protocol（路由信息协议）

SLB Server Load Balancing（服务器负载均衡）

SNMP Simple Network Management Protocol（简单网络管理协议）

STP Spanning-Tree Protocol（生成树协议）

TCP/IP Transmission Control Protocol/Internet Protocol

UDP User Diagram Protocal（用户报文协议）

UPS Uninterruptible Power Supply（不间断电源）

VLAN Virtual Local Area Network（虚拟局域网）

VPN Virtual Private Network（虚拟私有网）

VRRP Virtual Router Redundancy Protocol（虚拟路由冗余协议）

WAN　Wide Area Network（广域网）

WINS　Windows Internet Name Service（Windows 网际名字服务）。是微软开发的名字服务系统。

致　谢

在《指南》和《规范》任务提出和完成的整个过程中，相继得到了以下多家厂商、集成商的大力支持及技术方面的指导与帮助，在此表示感谢！

国际商业机器全球服务（中国）有限公司

美国康普国际控股有限公司北京办事处

微软(中国)有限公司

中国网通(集团)有限公司北京市分公司

北京联信永益科技有限公司

北京博望恒信智能系统有限公司

杭州华三通信技术有限公司

北京金山软件有限公司

航天四创科技有限责任公司