



思科中小型医院网络和应用解决方案



思科大中华区合作伙伴事业部

2010 年 12 月

目 录

第一章 概述.....	3
第二章 中小型医院信息化状况及发展	6
一、中小型医院信息化建设状况	6
二、中小型医院信息化应用及发展	7
第三章 中小型医院基础网络解决方案	10
一、中小型医院的网络需求	10
二、医疗级骨干网络解决方案	11
三、中小型医院接入解决方案	16
四、思科中小型医院基础网络设备参考	17
第四章 中小型医院网络安全保障解决方案.....	19
一、中小型医院的网络安全现状及挑战.....	19
二、构建安全的基础网络平台	19
三、内网安全与网络出口安全解决方案.....	23
四、安全的医疗分支机构解决方案	29
五、医院网络安全管理解决方案	32
六、思科网络安全解决方案优势	35
第五章 中小型医院无线网络及应用解决方案.....	36
一、中小型医院的无线需求	36
二、中小型医院的无线应用	36
三、思科无线解决方案优势	38
四、思科无线解决方案设备参考	45
第六章 中小型医院高效协作解决方案	47
一、中小型医院协作应用	47
二、思科协作解决方案设备参考	60
第七章 思科统一计算在医疗行业的应用	62
第八章 结束语：医疗行业用户为什么选择思科.....	67

第一章 概述

近二十年，我国医疗行业飞速发展，到目前为止全国各级别的医院大约 22000 家，其中三甲级别医院超过 1000 家占全部医院的大约 5.5%，二级医院超过了 5000 家约占 27%，一级医院超过 3000 家约占 14%，其他类型的医院超过 10000 家约占到 54.5%。可见二级以下的医院占了绝大的数量，随着民办、私立以及外资医院的增加，这个比例可能仍呈上升趋势。

随着计算机网络通讯技术的快速发展，医院信息化建设成为深化医疗体制改革的必要条件，成为医院改革发展、提高自身管理水平的有效手段，也是衡量现代化医院管理的重要内容。通过计算机网络技术途径，可以实现医院数字化建设，提升医院形象，增强医院整体竞争实力，为医院带来良好的社会效益、经济效益和文化效益。

在国家公布的《2006—2020 年国家信息化发展战略》中，对医疗卫生信息化建设提出的要求是：完善覆盖全国、快捷高效的公共卫生信息系统；增强防疫监控、应急处置和救治能力；推进医疗服务信息化，改进医院管理，开展远程医疗；统筹规划电子病历，促进医疗、医药和医保机构的信息共享和业务协同，支持医疗体制改革。

医疗信息化发展要经历三个阶段：医院管理信息化（HIS）阶段、临床管理信息化（CIS）阶段、局域医疗卫生服务（GMIS）阶段。HIS 阶段分为部门级的信息化管理和全院的信息化管理，是最初级的阶段。CIS 是以病人的电子病历为核心的信息化管理，要求医院的工作人员都有终端设备，信息处理无纸化，医院之间实现联网，电子病历等信息可在网上传递。GMIS 阶段即在社区以及偏远地区实现远程医疗信息资源共享。

虽然大型医院早已实施了较为完备的医疗信息化系统，可是，由于地域上的距离和网络发展的不平衡性，下属各地区、医院、医保定点网络之间缺少互联互通，各网络信息系统不能及时共享，造成网络的割裂和医疗信息的孤岛。一些地区人民医院的疾病诊断、检测设备相当落后，时常延误患者的诊治。当我们看到医院信息系统建设快速发展的同时，医疗行业信息化面临着前所未有的挑战和发展机会。医疗行业面临的主要挑战为：

- 医疗资源不足且分布不均，来自患者的直接反应主要是挂号难等问题；
- 医院运营成本高，来自患者的直接反应主要是看病花费高；
- 看病有风险，来自患者的直接反应主要是担心误诊和用错药等医疗事故发生在自己的身上。

信息网络技术由于具有以下特点，因而成为解决医院所面临的问题提供了有

力的工具：

- 提高医护工作效率；
- 降低医院运营成本；
- 提高医疗工作准确度等。

提高医护工作效率，就是使医院可以在原有专家医护资源不变的情况下，通过信息化的手段提高看病的效率，单位时间内能够为更多的患者服务，从而缓解看病难的问题；

降低医院运营成本，就是通过信息化的手段使医院在运营的过程中减少因为大量的手工记录，纸张的消耗和重复检查带来的成本，从而能够做到缓解看病贵的问题，或者是使医院的有限资金使用得更有效率；

提高医疗工作准确度，就是要通过信息化的手段降低事故风险，提高医疗服务质量，从而达到提高患者满意度的目的。

目前，总体来看，医疗卫生行业信息化建设已取得显著的进展，呈现明显的上升势头，信息化投资力度不断加大，医院信息化已进入实质阶段，是近几年信息化建设发展最为迅速的领域之一。对于中小型医院而言，随着现有规模的不断变大，医院的业务量和业务类型都发生了新的变化，不仅业务量较从前大幅上升，针对多种业务的整合也是对新网络平台提出的要求，传统的简单办公网络已经不能满足多业务的要求。

总之，中小型医院目前亟待完善以病人为中心，以医护人员为主体的高效医疗服务体系，在创建人民满意医院、构建和谐医疗的同时改善医院的财务状况。思科在大量医疗行业信息化建设实践的基础上，总结国内中小型医院信息化建设的经验，结合国内中小型医院的发展现状，推出了适宜于我国中小型医院的网络和应用整体解决方案，为中小型医院构建安全、可靠、承载生命信息的数字化医疗信息网络和应用平台。

目前中小型医院的信息化应用主要分为两大类：

- 数字化的医疗应用
- 高质量的医疗服务

数字化的医疗应用：主要包括医院管理信息系统和临床管理信息系统，如 HIS, OA, 住院管理、药房管理等，以及，一些医院准备实施的电子病历 (EMR)、电子处方，也有些医院在计划实施的小型医学影像存储与传输 (PACS) 系统等，以上这些医疗核心业务应用要求医院的网络具有较高的可靠性和安全性，以保证医院信息系统及其他办公统计应用能够安全、高速、不间断地运行，并能够灵活的扩充网络容量及网络服务，实现多种方式的接入，以适应未来扩大网络规模，

以及接入模式变化的需求。

高质量的医疗服务：包括护士呼叫、医疗导诊以及患者与家属的无线上网服务等，这些应用在中小型医疗网络上也将有效地发挥作用，因此现在的中小型医院只有基础网络连接是不能够满足医院业务的全面要求的，思科中小型医院网络和应用解决方案在基础网络之上有机地整合了思科统一无线网络解决方案和思科统一通信解决方案。

随着中小型医院信息化的迅猛发展，和 mini PACS 等新应用的实施，医院对服务器的性能及扩展性的要求也越来越高，基于思科统一计算系统的数据中心解决方案也成为思科中小型医院网络和应用解决方案的一个新的重要的组成部分。

下文将对思科中小型医院网络和应用解决方案进行较为详细的描述，主要包括：

- 中小型医院信息化应用及服务
- 中小型医院基础网络解决方案
- 中小型医院网络安全保障解决方案
- 中小型医院无线网络及应用解决方案
- 中小型医院高效协作解决方案
- 思科统一计算系统应用解决方案

详细信息欢迎垂询思科区域中小企业客户经理和中小企业客户技术支持工程师，或参考思科网站：

- **English: www.cisco.com**
- **中文: www.cisco.com.cn**

第二章 中小型医院信息化状况及发展

一、 中小型医院信息化建设状况

目前，我国医院在信息化建设的探索过程中，与大型三甲医院相比，中小型医院的信息化建设相对滞后与缓慢，其主要原因在于以下三个方面：

（1）医院领导重视不足，对信息化管理缺乏前瞻性；

管理的透明化造成对一些中层干部和他们的小群体的“局部利益”的侵犯，或者因原有工作方式的改变带来的不适应，势必使他们在思想上产生抵触情绪。这种错误思想、不良情绪将严重阻碍信息化建设的进行。

（2）医院的财力有限，资金投入不足；

大医院资金较为充裕，信息化程度较高，而小医院缺乏资金，信息化建设相对滞后。中小型医院往往由于经营的压力，更愿意投资购买一些可以立即产出效益的医疗设备，如CT机、麻醉机等，而不愿意在不能直接产生经济效益的信息系统上投入巨资。

（3）专业技术人才的缺乏。

对信息技术人员队伍建设要有开拓性认识，在我国医院信息化过程中，现在的信息化专业技术人才无论从数量上还是质量上，都不能满足医院的需求。尤其是既懂IT、又懂医学以及医院管理的复合型人才更是缺乏。

然而，中小型医院的IT建设，相比很多大医院，更加灵活。很多大医院虽然IT投入比较大，但是以前都是分步骤上系统，信息孤岛比较严重。现在要将所有系统整合到一起或重新建设，都面临很大的问题，相比之下，中小型医院更加灵活，信息化更加容易被贯彻执行。

对于大多数中小型医院，在社区医疗中心或乡镇卫生院和大型综合性医院的双重夹击下，要解决医院的经营问题，就需要医院在业务和服务上有所创新。从IT应用入手，结合医院业务的需求，加大信息化上的投入，让信息系统真正发挥作用。

IT技术对医院的帮助作用可以从三个方面体现。首先是效率的提高。系统的应用改变了传统的医院工作流程，通过信息交互和信息处理、采集和利用，使医院各环节运行效率加快。其次是医疗质量的增强。通过信息化手段加强医疗各环节的规范性，减少医疗差错，保证医疗质量。第三是服务方式的增多。用更为便捷的手段和流程，为医院管理者、医护人员以及病人解决了原来无法解决的问题，增加各种新的服务方式。

通过 IT 手段不仅加强成本控制和精细化管理，而且改善医疗服务，以医患为中心，在 IT 应用的基础上，引进新技术、新服务，从而打造医院的核心竞争力。

二、 中小型医院信息化应用及发展

目前，总体来看，医疗卫生行业信息化建设已取得显著的进展，呈现明显的上升势头。2009 年全国两会以后，信息化投资力度不断加大。大型医院的信息化已经进入整合阶段，未来会保持稳定的发展速度，数字化医院集成平台会逐步建立；中小型医院的信息化建设进入快速发展期，各类软硬件产品保持快速增长，社区卫生和公共卫生管理信息化也呈现出加速发展的态势。医院信息化已进入实质阶段，是近几年信息化建设发展最为迅速的领域之一。

但是，从全国范围来看，医疗系统的信息化还远未实现，还需要大量的网络建设与应用集成工程建设工作。随着以电子病历为中心的 CIS 系统的推广，各种医疗单位之间联网的需求将更为迫切，因为只有高带宽的网络才能实现医疗数字影像等大容量信息的畅通传输，只有安全级别高的网络才能确保电子病历的高保密性，确保病人的隐私被保护和处方的安全性。

而且，病人的不断增多以及医疗管理技术的落后，信息化程度的不够深入和全面，致使许多医院的医务人员面临着越来越大的压力。一方面他们需要在更短的时间内处置更多的病人，而另一方面医院的经济效益却在不断地下滑、因医疗事故引发的医疗纠纷日趋增多。为了缓解医务人员的这些压力，目前许多医院都在积极加大信息化系统建设，具体到医院信息化工程建设上，从五个方面逐步深入加强完善，即医院信息系统（HIS）、办公管理系统（OA）、检验系统（LIS）、医学影像系统（PACS）、远程医疗系统建设，借助网络科技手段提高医疗服务质量和医务管理水平，提高医院的经济效益。

医院信息系统（HIS）

完整的 HIS 系统实现了信息的全过程追踪和动态管理，从而做到了简化患者的诊疗过程，优化就诊环境，改变目前排队、等候时间长、秩序混乱的局面。HIS 系统在医院中的功能包括门诊管理、住院管理、病案管理、药品管理、物资管理、人事管理、财务核算等等，覆盖医院的业务工作、管理活动和经营决策等环节，为现代医院的信息化提供了全方位、全过程的整体支持。

实验室信息管理系统（LIS）

随着医院临床检验工作的日趋自动化、流水化、电子化，众多医院和检验科建立了实验室信息管理系统（LIS）。检验完成后迅速反馈到临床，节约了时间和工时，从而避免了病人和医务人员拿着检验单满医院乱跑的“繁忙”景象。

门诊导诊多媒体查询系统

使病人能了解医院各科室的分布和各专业、专家门诊的出诊时间，能查询到实时的住院、门诊费用以及各项检查等的费用，增加了医院收费的透明度，为病人提供了快捷方便的服务方式。

电子病历系统

电子病历系统是以电子病历和医嘱为核心，病人的所有信息都必须汇到电子病历之中，电子病历的内容非常丰富，包括病人入院记录、病人临床记录、外科记录、生产记录、病人病情描述，检验检查结果，病情客观诊断等等。

图像存储于通信系统

图像存储于通信系统（PACS）是医院用于管理医疗设备如 CT、MR、彩超等医学图像的信息系统，它支持在医院内部的所有关于图像的活动，集成了医疗设备、图像存储和分发，数字图像在重要诊断和会诊时的显示、图像归档，以及外部信息系统，提高部门内医疗设备的使用效率，可帮助医院的其他部门，特别是急诊室和监护室及时获得放射、影像部门生成的图像，并可进行远程图像传输和显示。

远程医疗

远程医疗是指医学专家利用电子通讯以及多媒体技术实现远距离医学检测、监护、咨询、急救、保健、诊断、治疗以及远距离教育和管理等，是近年来发展起来的一种医疗活动方式，它解决了医疗资源越来越不平衡的状况，既节省了病员费用，也是病员得到了一流服务，并且极大地提高了医院的信誉，由此而导致了数码医院的建立。

远程医疗系统它具有获取、传输、处理和显示图像、图形、语言、文字和生理信息的功能，通过多媒体、高速移动通讯网络、微电子医疗设备实现远程医疗。根据它的临床应用，远程医疗又可分为远程监护、远程会诊、远程诊疗和远程教育等。

当前，中小型医院的信息化应用主要包括两个方面：医院管理信息化和临床管理信息化。

医院管理信息化：

包括三个方面：1、医院内部方面，实现医院内部的行政、财务、HR、图书馆、药房、床位、医疗器械等等的电子化管理；2、医院与上下游供应商方面，实现药品、医疗器械、耗用品的采购的电子化管理；3、医院和用户即病人方面，实现收费、社保医疗卡划账、信息查询等的电子化管理。这三个方面相辅相成，构成整个医院的 ERP 系统。

临床管理信息化：

通过医疗资讯系统、医学影像系统、医疗器械数据采集系统等先进技术实现电子病历、医疗信息无纸化传递。这样能够保证病历信息的快速流通，减少病历数据的出错率，最大限度的治病救人。不但如此，电子病历的建立还为建设全社会的、高质量的、公正的个人医疗保健信息数据库提供了可能，有助于医疗机构由医疗卫生事业向医疗卫生保健事业的演进。

根据目前医疗系统的信息化水平，中小型医院的信息化建设应以实用性为主，在此基础上兼顾先进性、可扩展性和可管理性。主要目标是建设医院内部的快速可靠的计算机网络通讯系统，实现医院管理信息化和临床管理信息化。将传统的医院建设成为电子医院，用电子化信息取代传统的信息，提高工作效率。建设医院的 Internet 门户网站，宣传医院，向公众提供网上门诊预约服务等等。

对外改进病人服务，例如解决群众反映最大的看病等待时间长和付款取药时间长的问題，并能够提供更多的新业务；对内提高医院内部的效率，提高诊疗的成功率。

第三章 中小型医院基础网络解决方案

中小型医院的网络上运行着医院重要的核心业务应用系统,如医院信息系统(HIS)、和临床信息系统等。这些系统关系到人们的生命安全和身体健康,关系到医院的声誉和收入,因此对网络的可靠性具有较高的要求。

一、 中小型医院的网络需求

我们需要准备一个怎样的网络,才能满足中小医院对网络的需求?让我们先从小型医院的应用系统看起。纵观医疗信息化的应用,大致可以分为三个方面:管理信息系统、临床信息系统、其他信息系统:

管理信息系统的应用特点是以文字、简单图形信息为主,虽然数据量不大,但对于基础架构需要比较高的可靠性和安全性高,对服务质量也有一定的要求。相比之下,临床信息系统的应用则更为丰富。除一般文本信息外,医疗应用数据包含大量图形、视频、语音信息,要求安全、可靠、保证服务质量和高性能,需要同时支持语音、视频和数据等多种业务,又要方便以后的扩展。在某些关键应用上,对于服务质量、高性能、高可用性又提出了更高的要求。

其他信息系统涉及对外连接,用户对远程资源的访问控制以及广域网链路服务质量是关键,因而对系统可靠性和安全性要求较高,需要同时支持语音、视频和数据等多种业务。

中小型医院的信息系统有着一些共同的特点:医院信息管理系统(HIS)多采用客户机/服务器结构;程序模块化设计,通常包括门诊部分、住院部分、手术医技部分、药房药库部分、后勤仓库部分、综合查询部分,以及系统管理员和字典维护等,信息以数字、文字为主,图片、声音、视频图像较少;节点相对较少,分布相对集中;域结构简单,多为单域 构;与 Internet 网连接的电脑不多,仅限于个别行政部门。

中小型医院的网络系统建设主要实现以下几个目标:实现信息共享,为医院信息管理系统、办公软件等应用程序的运行,提供安全、可靠、高速的平台;通过路由实现医保联网及 Internet 网的联接;建立内部网站,培养医院文化,降低办公成本,提高办公效率;实现网管和网络实时监控功能,减少网络故障发生率,缩短故障处理时间。

中小型医院网络规模虽然不如大型医院庞大,但信息点数量也达到了几百个,网络覆盖范围包括医生诊室、办公室、挂号部门、药品发放部门、财务部门以及病房等,并且随着网络应用的丰富和医疗业务的扩展,网络规模将不断扩大,考虑到中小型医院经济实力和组网成本,因此,中小型医院网络系统的建设应以实

用性为主，在此基础上兼顾先进性，优越的扩展能力可管理性和升级空间，保护医院投资，减少重复建设。中小型医院的网络系统建设应满足以下 5 个方面的需求：

- (1) 建立高速骨干网络，保证各楼宇、各网段之间线速无阻塞的数据交换；
- (2) 良好的兼容性，保障医院各管理系统软件的正常运行；
- (3) 可进行医院日常业务的处理，如：门诊及住院管理、药品管理、电子病案管理等，还需要实现医院的管理层信息管理。
- (4) 能够灵活的扩充网络容量及网络服务，可以实现多种方式的接入，以适应未来扩大网络规模，以及接入模式变化的需求；
- (5) 能够完成一些基本的网管和实时监控功能。

二、 医疗级骨干网络解决方案

高可靠性是医疗网络的首要关注点。随着医疗网络应用越来越多地推广到临床实践当中，任何网络中断事件都可能带来很严重的后果，网络的可用性将直接影响到医院的经济效益，社会效益和管理水平；未来的医疗网络还将会承载越来越多的新应用，如部署 IP 电话和无线移动医疗服务等，这些都对网络的可用性、数据传输的可靠性和快速响应能力提出很高的要求。

此外，在高速传输方面，对于影像科室/临床科室这些重要的部门，由于涉及医学影像的传输，又是医疗服务的关键，适宜采用桌面千兆、主干万兆双机备份的交换连接；对于收费、挂号等需要运行 HIS/RIS/LIS 的流程管理部门，可以采用桌面千兆、主干千兆双机备份的交换连接；对于其它对网络可靠性要求不高的科室，可以采用桌面百兆、主干千兆的解决方案，但是并不是必须采用双机备份的解决方案。

提高网络系统的可靠性，一方面要提高构成网络系统的各设备本身的可靠性，如核心层、汇聚层、接入层设备以及链路的可靠性。另一方面，要从网络系统的设计着手，要使网络系统的部件工作在正常状态下，没有过载超负荷等现象的发生。三，还要实现冗余贮备，即使网络系统有个别设备或链路出现故障仍能正常工作；譬如提供备用电源等。当然冗余设备有可能增加系统的复杂性和成本，但是如果设计得合理，在成本增加不多的情况下，使系统的可靠性有很大的提高，是完全值得的。

目前一部分医院网络现状主要呈现以下特点：

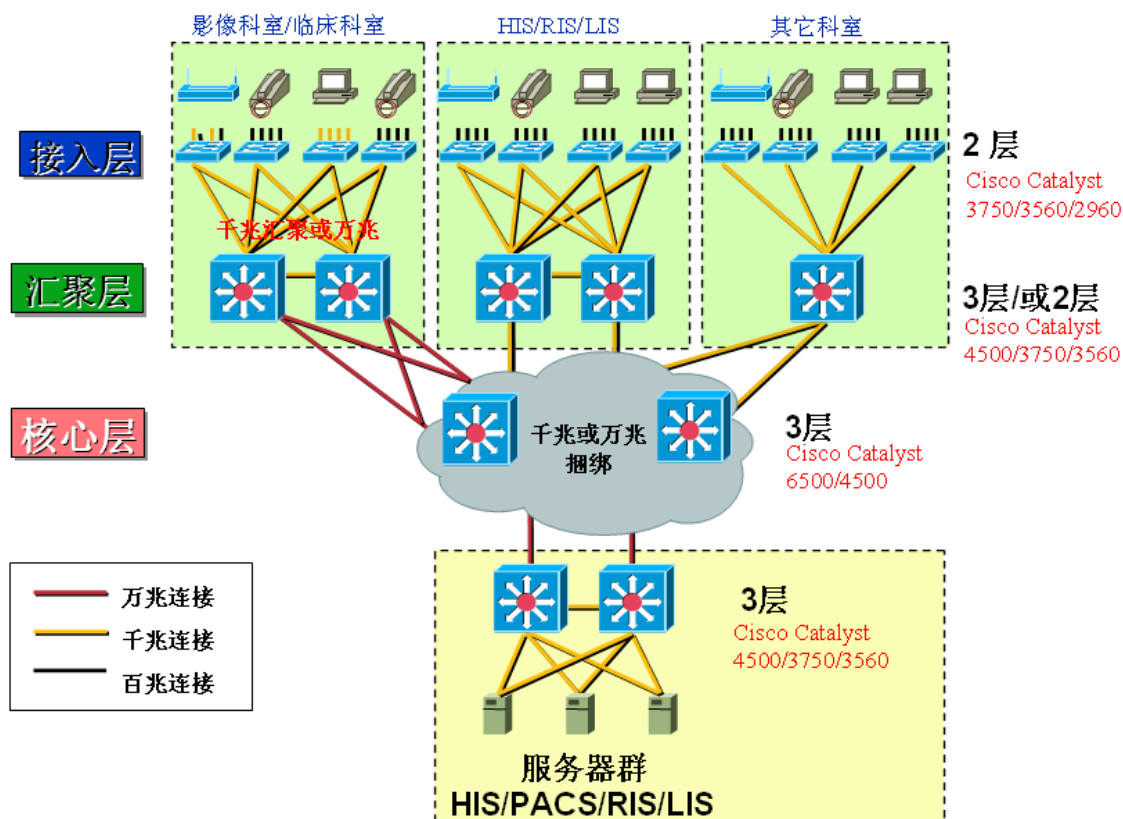
- 模块化，多层架构；
 - 核心层、汇聚层和接入层架构 与 核心和接入层架构 相结合

- 双核心交换机（热备或冷备）
- 单汇聚交换机（增加单点故障）和双汇聚交换机相结合
- 核心层具有路由功能，部分汇聚层具有路由功能；
- 汇聚层或核心层负载均衡；
- 少量 VLAN 跨越（部分网络没有划分 VLAN）；
- 千兆和百兆相结合；

思科医疗级网络解决方案主要通过三个途径帮助医院实现网络的高可靠性，尤其是对于承担医疗核心业务的内网，一是高可靠的医疗级网络架构设计；二是思科保证医疗级网络业务高可靠运行的独特网络技术；三是建立医疗数据中心的存储整合和数据灾备。

为此，思科建议的典型医疗级网络架构如下图所示。网络设计为包括核心层、汇聚层和接入层的多层模块化架构，网络骨干为部分万兆或千兆，百兆到桌面，部分千兆到桌面，关键部位采用冗余结构，核心交换机和汇聚交换机双备份。核心层和汇聚层均有路由功能，接入层具有交换或路由功能，实施负载均衡和冗余备份，VLAN 尽量终结在本地以缩小故障域，整个网络万兆、千兆和百兆相结合。这种设计建议来自思科美国总部的顾问工程师小组的实验室研究和用户最佳实践的结果，这种架构的主要优势在于其层次结构和模块性，模块化设计允许您通过推行确定性的流量模式来轻松扩展、了解并排除网络故障。

高可靠，部分万兆骨干，千兆/百兆到桌面，关键部位冗余结构



(图) 医院网络架构新趋势：多层模块化解决方案

在层次化设计中，特定设备的容量、特性和功能均针对其网络位置和作用进行了优化，以提高可扩展性及稳定性。当流量通过层次化结构中的收敛点，沿着接入层-汇聚层-核心层传输时，流量数量及其相关的带宽要求都随之增加。层次化设计每一层的功能都很分明，无需全部网络节点互联的全网状网络。

模块化网络的组件易于复制、重新设计并扩展，无需每次添加或拆除模块时都重新设计整个网络。您可以运行或中断任何组件的运行，而不会影响网络的其他部分。这种功能可促进排障、故障隔离和网络管理。

该架构已经经过思科在众多医疗行业用户和园区网用户验证，能够提供最大限度的可靠性。

仅仅把网络按照以上架构连接起来是远远不够的，还需要网络架构中的每个节点设备都具有高可靠的内在品质，在这一点上，思科的网络设备在各个对可靠性要求比较高的如：医院，银行，证券等行业都具有非常好的口碑。同时在不同层次的设备上还需要有基于国际标准的，以及思科独特的保证医疗业务高可靠运行的网络功能，举例如下：

(1) 核心层

在典型的层次化模式中，组件间通过核心层互联，核心用作网络骨干。鉴于各组件都依赖核心进行连接，因此，核心必须速度很快且永续性极高。现在的硬件加速系统具备以线速提供复杂业务的潜能。然而，应在网络核心采用“越简单越好”的方法。最简洁的核心配置可降低配置复杂性，从而减少出现运行错误的几率。

虽然通过全网状或高度网状拓扑也可实现冗余，但此类设计在链路或节点发生故障时不容易提供一致的收敛。同时，全网状设计也存在对等和邻接问题，使路由难以配置和扩展。此外，随着网络的增长或变化，大量的端口也增加了不必要的成本和复杂性。以下是需要谨记的其他主要设计问题：

- 将核心层设计为只使用硬件加速业务的高速第 3 层 (L3) 交换环境。第 3 层核心设计优于第 2 层和其他设计，因为它：
 - 在发生链路或节点故障时提供更快的收敛速度。
 - 通过减少路由邻接关系和网状拓扑提高了可扩展性。
 - 提高了带宽利用率。
- 尽量在核心中使用冗余的点到点 L3 互联（三角形，不是正方形），因为这种设计可产生最快速、最确定的收敛结果。
- 避免 L2 环路和 L2 冗余的复杂性，如生成树协议(STP) 和 L3 组件对等体之间的间接故障检测。
- 采用模块化的操作系统，使得局部的软件故障不会影响整机的运行。软件的升级也可以在局部软件模块进行，而不必为升级软件等维护工作是核心交换机停止工作，影响全网的运行。

(2) 汇聚层

汇聚层汇聚来自接入层的节点，保护核心不受高密度对等关系的影响。此外，汇聚层还创建故障边界，在接入层发生故障时提供逻辑隔离点。汇聚层通常以 L3 交换机的形式部署，针对网络核心连接使用 L3 交换，对接入层连接使用 L2 服务。负载均衡、服务质量(QoS)和易于设置等都是汇聚层的主要考虑因素。

汇聚层的高可用性通过两条等成本路径来提供，包括从汇聚层到核心以及从接入层到汇聚层的链路，可在链路或节点发生故障时提供确定性的快速收敛。当冗余路径存在时，故障切换主要依赖硬件链路故障检测，而不是基于定时器的软件故障检测。基于这些功能（在硬件中实施）的收敛是最具确定性的。

L3 等成本负载分担允许同时利用从核心到汇聚层的两条上行链路。汇聚层使用网关负载均衡协议 (GLBP)、热备份路由器协议 (HSRP) 或虚拟路由器冗余协议 (VRRP) 提供缺省的网关冗余。当一个汇聚层节点发生故障或被拆除时，

不会影响端点与缺省网关的连接。

您可以通过多种方式在接入层到汇聚层的上行链路间实现负载平衡,但使用 GLBP 是最简单的方法。GLBP 提供了类似 HSRP 的冗余和故障防护,还允许向接入层设备轮流分配汇聚层设备作为缺省网关,以便端点向两个之中的一个汇聚层节点发送流量。

(3) 接入层

接入层是边缘设备、终端站和 IP 电话接入网络的第一层。接入层中的交换机连接两个单独的汇聚层交换机以实现冗余。如果它与汇聚层交换机之间是 L3 连接,则不会出现环路,所有上行链路都将有效转发流量。

在接入层,通常会划分 VLAN,目的在于:一是提高网络安全性,不同 VLAN 的数据不能自由交流,需要接受第三层的检验,因此,在一定程度上加强了虚网间的隔离,有效防止外部用户入侵,提高了安全性。二是隔离广播信息,划分 VLAN 后,广播域缩小,有利于改善网络性能,能够将广播风暴控制在一个 VLAN 内部,同时使网络管理趋于简单。三是增强网络应用的灵活性,VLAN 是在一个有多台交换机的局域网中统一设定的,这使得用户可以不受所连交换机的限制,不论用户节点移动到局域网中哪一台交换机上,只要仍属于原来的虚网,则应用环境没有任何改变。在划分 VLAN 时,要考虑 VLAN 对于网络流量的影响,单个 VLAN 不宜过大。

健壮的接入层提供以下主要特性:

- 许多软硬件属性支持的高可用性 (HA)。
- IP 电话和无线访问点的馈线供电(POE)允许客户将话音融合到数据网络中,并为用户提供漫游 WLAN 访问。
- 基础服务。

支持高可用性的接入层的软硬件属性包括:

- 使用冗余交换管理引擎和冗余电源获得的系统级冗余,为关键用户群提供高可用性。
- 使用到冗余系统(使用 GLBP、HSRP 或 VRRP 的汇聚层交换机)的双倍连接获得的缺省网关冗余,支持在汇聚层的主备交换机间快速实现故障切换。
- 链路汇聚(以太网通道或 802.3ad)等操作系统高可用特性,提供更高的带宽利用率,同时降低复杂性。
- 使用 QoS 为关键任务网络流量分发优先级,从而尽量靠近网络入口对流量进行分类和排队。

- 安全服务，通过配置 802.1x、端口安全性、DHCP 侦听、动态 ARP 检查及 IP 源保护等工具来增加安全性，从而更有效地防止非法网络访问。

三、 中小型医院接入解决方案

中小型医院的网络解决方案主要特点有：骨干连接采用 1000M，10/100M 连接桌面用户，线速核心第三层交换，使路由器专注于处理广域网流量，采用光缆支持较长距离，可做办公楼间连接，更多的网络插槽提供更强更灵活的扩展能力等。

网络核心层选用 Cisco Catalyst 6500 或 4500 作为核心交换机，提供多个千兆光纤模块，并与各个大楼的中心交换机相连，使整个网络形成千兆主干。另外，中心交换机在满足用户目前需求的基础上，将来还可接入万兆接口模块，充分实现了医院对网络的可扩展要求。

在中小型医院的网络汇聚层，选用 Catalyst 3750 或 3560 交换机，通过光纤双千兆链路分别上连到核心交换机 Catalyst 6500 或 4500，任意一条链路故障不影响网络的正常运行。

在接入层，分别在每楼层放置 Catalyst 3560 或 2960 等交换机，与汇聚交换机相连，支持 10/100/1000 Mbps 连接到医院部门和办公用 PC 机，并且支持堆叠。另外，接入层还可以采用思科精睿 300 系列交换机。

思科 300 系列由多个固定配置网管型以太网交换机构成。其型号包括 8 到 48 个端口的快速以太网连接以及 10 到 52 个端口的千兆以太网连接，为构建适合于中小型医院的接入网络提供了灵活多变的选择。思科 300 系列交换机均具备针对数据、语音、安全、以及无线技术的高级安全管理功能及各项网络特征，同时，还具有易于部署和配置的特点，能够充分发挥受控网络服务的优势。

■ 先进性：采用先进、成熟的网络通信技术，使网络轻松支持数据、语音、视像等多媒体应用，通过基于交换的技术替代传统的基于路由的技术，既满足了医院多种类数据的传输需求，也确保了网络技术和网络产品几年内不落后。

■ 安全性：信息系统安全的中心任务是保证信息网络的畅通，确保授权实体经过该网络安全地获取信息，并保证该信息的完整和可靠。网络系统提供了全面的安全策略，通过采用防火墙、应用网络优化原理等手段，加强了网络的可靠性。网络中所有交换机都支持 802.1Q 和 VLAN 虚拟网络技术。可以方便地根据 IP 地址、TCP/UDP 端口号及协议类型进行数据过滤，保护了网络资源的安全。RV082 和 RV042 可以提供安全的 IPSec VPN 连接，为医院、药房与医保机构之间提供专用的虚拟安全通道，保证医保信息的安全传递。

■ 灵活性：网络作为医院发展的辅助环境，需要随着医院业务的变化而变化，具备出色的需求适应能力。解决方案中的网络系统具有良好的扩展性，能够随着医院规模的扩大而实现网络规模的相应扩大，并能够针对医院业务的开展，进行系统的快速升级和改装，使医院的网络建设成为一项持续性的系统工程项目，从长远来看，十分有助于用户节约成本，避免不必要的浪费。建成后的网络帮助医院实现了内部财务系统的主机同本地市医保中心系统之间的连接，使医院能够在第一时间访问本地医保中心的主机，查看他们的财务状况与病人记录，从而能够轻松地完成对医保项目的管理工作。

四、 思科中小型医院基础网络设备参考

- 核心层（两台）

产品系列	产品描述
Catalyst 6500 系列交换机	模块化、机箱式、高端口密度交换机
Catalyst 4500 系列交换机	模块化、机箱式、高端口密度交换机

- 汇聚层（两台或者一台）

产品系列	产品描述
Catalyst 4500 系列交换机	模块化、机箱式、高端口密度交换机
Catalyst 3750-X 交换机	支持堆叠和万兆上行的智能三层交换机
Catalyst 3560-X 交换机	支持万兆上行的智能三层交换机
Catalyst 3750G/E 系列交换机	支持 10//100/1000M，GE/10G 上行的工作组交换机
Catalyst 3560G/E 系列交换机	支持 10//100/1000M，GE/10G 上行的工作组交换机

- 接入层（若干台）

产品系列	产品描述
Catalyst 3750-X 系列交换机	支持堆叠和万兆上行的智能三层交换机
Catalyst 3560-X 系列交换机	支持万兆上行的智能三层交换机
Catalyst 3750G/E 系列交换机	支持 10//100/1000M, GE/10G 上行的工作组交换机
Catalyst 3560G/E 系列交换机	支持 10//100/1000M, GE/10G 上行的工作组交换机
Catalyst 2960S 系列交换机	支持堆叠、万兆上行的千兆交换机
Catalyst 2960 系列交换机	支持千兆上行的百兆交换机
SG 300 系列交换机	支持静态路由的可网管千兆交换机
SF 300 系列交换机	支持静态路由的可网管百兆交换机

- 远程 VPN 接入路由器

产品系列	产品描述
RV082 路由器	支持 IPSec VPN 的宽带路由器
RV042 路由器	支持 IPSec VPN 的宽带路由器

详细信息欢迎垂询思科区域中小企业客户经理和中小企业客户技术支持工程师，或参考思科网站：

- English: www.cisco.com
- 中文: www.cisco.com.cn

第四章 中小型医院网络安全保障解决方案

一、 中小型医院的网络安全现状及挑战

现阶段，医院信息系统正在变成医疗体系结构中不可或缺的基础架构。该架构的网络安全和数据可用性变得异常重要。任何的网络不可达或数据丢失轻则降低患者的满意度，影响医院的信誉，重则引起医患纠纷、法律问题或社会问题。和其它行业的信息系统一样，医疗信息系统在日常运行中面临各种安全风险带来的安全应用事故。

当前，中小型医院在网络和应用系统保护方面均采取了一定的安全措施，例如在每个网络、应用系统分别部署了防火墙、访问控制设备；也可能在一定程度上实现了区域性的病毒防御，实现了病毒库的升级和防病毒客户端的监控和管理；采用系统账号管理、防病毒等方面具有一定流程。但在网络安全管理方面的流程相对比较薄弱，需要进一步进行加强；另外主要业务应用人员安全意识有待加强，日常业务处理中存在一定非安全操作情况，终端使用和接入情况复杂。此外，随着移动医疗应用越来越广泛的部署，以及依托互联网平台的远程医疗应用的日趋广泛，如何保障移动和远程应用的安全性也是一个重要的课题。

网络安全问题越演越烈，也为中小型或成长型的医疗机构带来另外一个挑战：如何利用较为有限的投资预算，解决当前最为迫切的安全威胁，同时也要预留先进性和可扩展能力，避免造成投资浪费。思科自防御网络的出现，为中小型医疗网络提供了由低级到高级不断发展、演进的安全解决方案，思科网络设备集成了独特的安全功能，以及各个安全设备的联动并主动进行防护，是思科自防御网络的具体实现。

基于思科自防御安全体系的建设指导思想，同时结合中小型医疗机构的安全现状，我们建议从以下几个方面构筑中小型医疗机构的安全体系。

二、 构建安全的基础网络平台

在诸多的局域网安全问题中，由于历史原因，令网络管理员感到最头痛的问题就是 IP 地址的管理；最担心的问题就是账号、密码的盗取以及信息的失窃和篡改；而最棘手的问题就是木马、蠕虫病毒爆发对网络造成的危害。据 CSI/FBI 计算机犯罪与安全调查显示，信息失窃已经成为当前最主要的犯罪。在造成经济损失的所有攻击中，有 75%都是来自于园区内部。这样，企业网络内部就必须采用更多创新方式来防止攻击，如果我们将网络中的所有端口看成潜在敌对实体获取通道的“端口防线”，网络管理员就必须知道这些潜在威胁都有哪些，以及

需要设置哪些安全功能来锁定这些端口并防止这些潜在的来自网络第二层的安全攻击。

网络第二层的攻击是网络安全攻击者最容易实施,也是最不容易被发现的安全威胁,它的目标是让网络失效或者通过获取诸如密码这样的敏感信息而危及网络用户的安全。因为任何一个合法用户都能获取一个以太网端口的访问权限,这些用户都有可能成为黑客,同时由于设计 OSI 模型的时候,允许不同通信层在相互不了解情况下也能进行工作,所以第二层的安全就变得至关重要。如果这一层受到黑客的攻击,网络安全将受到严重威胁,而且其他层之间的通信还会继续进行,同时任何用户都不会感觉到攻击已经危及应用层的信息安全。

所以,仅仅基于认证(如 IEEE 802.1x)和访问控制列表(ACL, Access Control Lists)的安全措施是无法防止来自网络第二层的安全攻击。一个经过认证的用户仍然可以有恶意,并可以很容易地执行本文提到的所有攻击。目前这类攻击和欺骗工具已经非常成熟和易用。

以上所提到的攻击和欺骗行为主要来自网络的第二层。在网络实际环境中,其来源可概括为两个途径:人为实施,病毒或蠕虫。人为实施通常是指使用一些黑客的工具对网络进行扫描和嗅探,获取管理帐户和相关密码,在网络上中安插木马,从而进行进一步窃取机密文件。攻击和欺骗过程往往比较隐蔽和安静,但对于信息安全要求高的企业危害是极大的。木马、蠕虫病毒的攻击不仅仅是攻击和欺骗,同时还会带来网络流量加大、设备 CPU 利用率过高、二层生成树环路、网络瘫痪等现象。

归纳前面提到的局域网目前普遍存在的安全问题,根据这些安全威胁的特征分析,这些攻击都来自于网络的第二层,主要包括以下几种:

- MAC 地址泛滥攻击
- DHCP 服务器欺骗攻击
- ARP 欺骗
- IP/MAC 地址欺骗

利用 Cisco Catalyst 交换机内部集成的安全特性,采用创新的方式在局域网上进行 IP 的地址管理、阻止网络的攻击并减少病毒的危害。Cisco Catalyst 智能交换系列的创新特性针对这类攻击提供了全面的解决方案,将发生在网络第二层的攻击阻止在通往内部网的第一入口处,主要基于下面的几个关键的技术。

- Port Security
- DHCP Snooping
- Dynamic ARP Inspection (DAI)

- IP Source Guard

我们可通过在思科交换机上组合运用和部署上述技术,从而防止在交换环境中的“中间人”攻击、MAC/CAM 攻击、DHCP 攻击、地址欺骗等,更具意义的是通过上面技术的部署可以简化地址管理,直接跟踪用户 IP 和对应的交换机端口,防止 IP 地址冲突。同时对于大多数具有地址扫描、欺骗等特征的病毒可以有有效的报警和隔离。

通过启用端口安全功能,可有效防止 MAC 地址泛洪攻击,网络管理员也可以静态设置每个端口所允许连接的合法 MAC 地址,实现设备级的安全授权。动态端口安全则设置端口允许合法 MAC 地址的数目,并以一定时间内所学习到的地址作为合法 MAC 地址。

通过配置 Port Security 可以控制:

- 端口上最大可以通过的 MAC 地址数量
- 端口上学习或通过哪些 MAC 地址
- 对于超过规定数量的 MAC 处理进行违背处理

端口上学习或通过哪些 MAC 地址,可以通过静态手工定义,也可以在交换机自动学习。交换机动态学习端口 MAC,直到指定的 MAC 地址数量,交换机关机后重新学习。目前较新的技术是 Sticky Port Security,交换机将学到的 mac 地址写到端口配置中,交换机重启后配置仍然存在。

对于超过规定数量的 MAC 处理进行处理一般有三种方式(针对交换机型号会有所不同):

- Shutdown: 端口关闭。
- Protect: 丢弃非法流量,不报警。
- Restrict: 丢弃非法流量,报警。

Catalyst 交换机可通过 DHCP Snooping 技术保证 DHCP 安全特性,通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息,这些信息是指来自不信任区域的 DHCP 信息。通过截取一个虚拟局域网内的 DHCP 信息,交换机可以在用户和 DHCP 服务器之间担任就像小型安全防火墙这样的角色,“DHCP 监听”功能基于动态地址分配建立了一个 DHCP 绑定表,并将该表存贮在交换机里。在没有 DHCP 的环境中,如数据中心,绑定条目可能被静态定义,每个 DHCP 绑定条目包含客户端地址(一个静态地址或者一个从 DHCP 服务器上获取的地址)、客户端 MAC 地址、端口、VLAN ID、租借时间、绑定类型(静态的或者动态的)。

通过部署动态 ARP 检查(DAI, Dynamic ARP Inspection)来帮助保证接

入交换机只传递“合法的”的 ARP 请求和应答信息。DHCP Snooping 监听绑定表包括 IP 地址与 MAC 地址的绑定信息并将其与特定的交换机端口相关联，动态 ARP 检测（DAI – Dynamic ARP Inspection）可以用来检查所有非信任端口的 ARP 请求和应答（主动式 ARP 和非主动式 ARP），确保应答来自真正的 ARP 所有者。Catalyst 交换机通过检查端口记录的 DHCP 绑定信息和 ARP 应答的 IP 地址决定是否真正的 ARP 所有者，不合法的 ARP 包将被删除。

DAI 配置针对 VLAN，对于同一 VLAN 内的接口可以开启 DAI 也可以关闭，如果 ARP 包从一个可信任的接口接收到，就不需要做任何检查，如果 ARP 包在一个不可信任的接口上接收到，该包就只能在绑定信息被证明合法的情况下才会被转发出去。这样，DHCP Snooping 对于 DAI 来说也成为必不可少的，DAI 是动态使用的，相连的客户端主机不需要进行任何设置上的改变。对于没有使用 DHCP 的服务器个别机器可以采用静态添加 DHCP 绑定表或 ARP access-list 实现。

另外，通过 DAI 可以控制某个端口的 ARP 请求报文频率。一旦 ARP 请求频率的频率超过预先设定的阈值，立即关闭该端口。该功能可以阻止网络扫描工具的使用，同时对有大量 ARP 报文特征的病毒或攻击也可以起到阻断作用。

除了 ARP 欺骗外，黑客经常使用的另一手法是 IP 地址欺骗。常见的欺骗种类有 MAC 欺骗、IP 欺骗、IP/MAC 欺骗，其目的一般为伪造身份或者获取针对 IP/MAC 的特权。Catalyst IP 源地址保护（IP Source Guard）功能打开后，可以根据 DHCP 侦听记录的 IP 绑定表动态产生 PVACL，强制来自此端口流量的源地址符合 DHCP 绑定表的记录，这样攻击者就无法通过假定一个合法用户的 IP 地址来实施攻击了，这个功能将只允许对拥有合法源地址的数据包进行转发，合法源地址是与 IP 地址绑定表保持一致的，它也是来源于 DHCP Snooping 绑定表。因此，DHCP Snooping 功能对于这个功能的动态实现也是必不可少的，对于那些没有用到 DHCP 的网络环境来说，该绑定表也可以静态配置。

IP Source Guard 不但可以配置成对 IP 地址的过滤也可以配置成对 MAC 地址的过滤，这样，就只有 IP 地址和 MAC 地址都于 DHCP Snooping 绑定表匹配的通信包才能够被允许传输。此时，必须将 IP 源地址保护 IP Source Guard 与端口安全 Port Security 功能共同使用，并且需要 DHCP 服务器支持 Option 82 时，才可以抵御 IP 地址 + MAC 地址的欺骗。

与 DAI 不同的是，DAI 仅仅检查 ARP 报文，IP Source Guard 对所有经过定义 IP Source Guard 检查的端口的报文都要检测源地址。

通过在交换机上配置 IP Source Guard，可以过滤掉非法的 IP/MAC 地址，包含用户故意修改的和病毒、攻击等造成的。同时解决了 IP 地址冲突的问题。

此外，在最新的 Catalyst 3750-X 和 Catalyst 3560-X 交换机内，还内置了

一系列全新的 TrustSec 安全技术。例如，采用基于 IEEE 802.1ae 标准的 MAC Security 技术，交换机在面向主机的端口上提供了对以太网数据在数据链路层的线速加密，以防止中间人攻击；支持包括 802.1x、MAC 认证旁路、Web 认证等多种认证方式为不同类型的接入终端提供一致的安全体验，等等。

以上所列的基础安全防护的功能，均内置在思科的 Catalyst 交换机内,无需另外购买。

方案涉及的主要 Catalyst 系列交换机包括：

产品系列	说明
Catalyst 3750-X	支持堆叠和万兆上行的智能三层交换机
Catalyst 3560-X	支持万兆上行的智能三层交换机
Catalyst 2960-S	支持堆叠、万兆上行和静态路由的交换机

此外，思科还提供了精睿系列交换机，通过基本的 802.1x 认证、基于 MAC 的端口安全、基于 MAC/IP 的访问控制列表（ACL）、私有 VLAN 边缘（PVE）等技术，专为入门级的小型医疗网络提供基础的安全网络接入服务。精睿交换机的主要系列包括：

产品系列	说明
Cisco SF 300	支持静态路由的可网管交换机
Cisco SLM224G2	支持基于 WEB 浏览器简单网管的二层交换机

三、 内网安全与网络出口安全解决方案

现在的网络面临多种多样的安全威胁，医院需要建立纵深防御体系来防止因某个部分的侵入而导致整个系统的崩溃。只有基于网络系统之间逻辑关联性和物理位置、功能特性，划分清楚的安全层次和安全区域，在部署安全产品和策略时，才可以定义清楚地安全策略和部署模式。安全保障包括网络基础设施、业务网、办公网、本地交换网、信息安全基础设施等多个保护区域。这些区域是一个紧密联系的整体，相互间既有纵向的纵深关系,又有横向的协作关系，每个范围都有

各自的安全目标和安全保障职责。积极防御、综合防范的方针为各个保护范围提供安全保障，有效地协调纵向和横向的关系，提高网络整体防御能力。

针对医院的网络系统，我们可以根据物理位置、功能区域、业务应用或者管理策略等等划分安全区域。不同的区域之间进行物理或逻辑隔离。物理隔离很简单，就是建立两套网络对应不同的应用或服务，最典型的就是医院业务网络和互联网访问网络的隔离。而对于内部各部门或应用来说，我们经常采用的是利用防火墙逻辑隔离的方法。

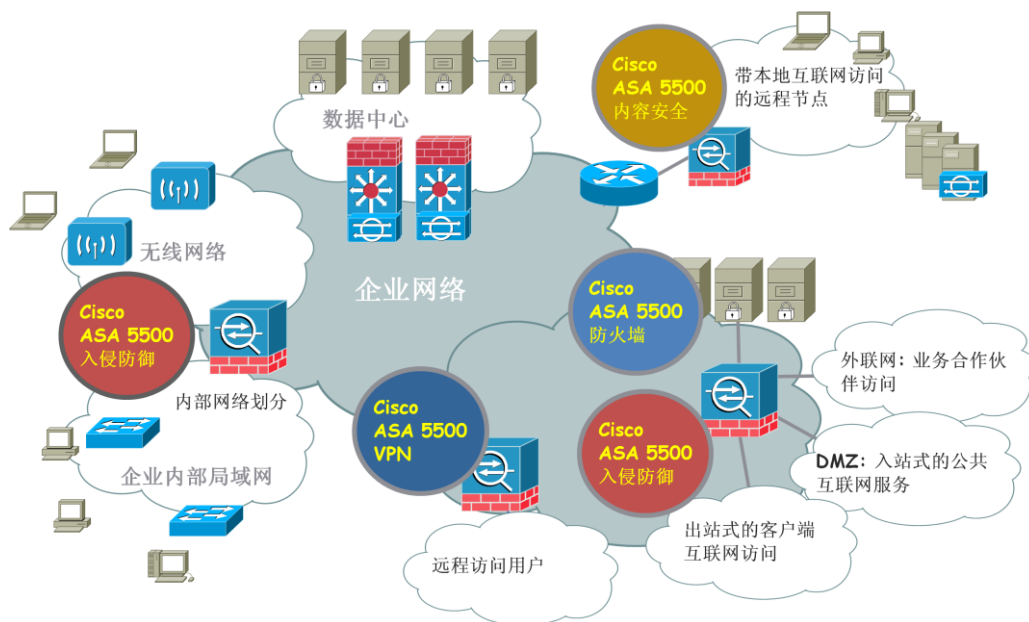
另一方面，互联网对各种规模的医院来说都十分重要。它带来了业务发展的新机遇。通过 VPN 连接，它使得医院可与合作伙伴和远程员工保持联系。但它也是将威胁带入医院网络的渠道，这些威胁可能会对医院造成重大影响：

- 病毒—可感染系统，使其停运，从而导致运行中断和收入损失
- 间谍软件和黑客—会导致公司数据丢失和因此引起法律问题
- 垃圾邮件和泄密—需要繁琐的处理过程，降低员工生产率
- 浏览与工作无关的网站—会导致员工生产率降低，并可能使公司承担法律责任
- 受感染的 VPN 流量—使威胁因素进入网络，中断业务

针对上述的安全威胁特点和需求状况，我们建议中小型医疗机构可以从以下几个方面部署思科的安全解决方案。

◇ 通过 Cisco ASA 5500 部署一体化安全解决方案

Cisco ASA 5500 系列提供了一体化安全解决方案，提供了一个易于使用、且具有医院需要的安全功能的全面安全解决方案，结合了防火墙、入侵保护、Anti-X 和 VPN 功能，您可对您的医院网络受到的保护充满信心。通过终止垃圾邮件、间谍软件和其他互联网威胁，员工生产率得到了提高。IT 人员也从处理病毒和间谍软件消除以及系统清洁任务中解放出来。您可集中精力发展业务，而无需为最新病毒和威胁担忧。



图：ASA 5500 系列一体化安全解决方案

Cisco® ASA 5500 系列为医院提供了全面的网关安全和 VPN 连接。凭借其集成的防火墙和 Anti-X 功能，Cisco ASA 5500 系列能在威胁进入网络和影响业务运营前，就在网关处将它们拦截在网络之外。这些服务也可扩展到远程接入用户，提供一条威胁防御 VPN 连接。

最值得信赖、广为部署的防火墙技术—Cisco ASA 5500 系列构建于 Cisco PIX 安全设备系列的基础之上，在阻挡不受欢迎的来访流量的同时，允许合法业务流量进入。凭借其应用控制功能，该解决方案可限制对等即时消息和恶意流量的传输，因为它们可能会导致安全漏洞，进而威胁到网络。

市场领先的 Anti-X 功能—通过内容安全和控制安全服务模块(CSC-SSM)提供的强大的 Anti-X 功能，Cisco ASA 5500 系列提供了全面保护所需的重要的网络周边安全性。

防间谍软件—阻止间谍软件通过互联网流量(HTTP 和 FTP)和电子邮件流量进入您的网络。通过在网关处阻拦间谍软件，使 IT 支持人员无需再进行昂贵的间谍软件清除过程，并提高员工生产率。

防垃圾邮件—有效地阻拦垃圾邮件，且误报率极低，有助于保持电子邮件效率，不影响与客户、供应商和合作伙伴的通信。

防病毒—屡获大奖的防病毒技术在您基础设施中最有效的地点—互联网网关处防御已知和未知攻击，保护您的内部网络资源。在周边清洁您的电子邮件和 Web 流量，即无需再进行耗费大量资源的恶意软件感染清除工作，有助于确保业务连续性。

防泄密— 确定针对泄密攻击的防盗窃保护，因此可防止员工无意间泄漏公

司或个人信息，以导致经济损失。

针对 Web 接入、电子邮件(SMTP 和 POP3)以及 FTP 的实时保护。即使机构的电子邮件已进行了保护，但许多员工仍会通过公司 PC 或笔记本电脑访问自己的个人电子邮件，从而为互联网威胁提供了另一个入点。同样，员工可能直接下载受到感染的程序或文件。在互联网网关对所有 Web 流量进行实时保护，可减少这一常被忽略的安全易损点。

URL 过滤—Web 和 URL 过滤可用于控制员工对于互联网的使用，阻止他们访问不适当的或与业务无关的网站，从而提高员工生产率，并减少因员工访问了不应访问的 Web 内容而承担法律责任的机会。

电子邮件内容过滤—电子邮件过滤减少了公司因收到通过电子邮件传输的攻击信息而承担法律责任的机会。过滤也有助于符合法律法规，可帮助机构达到 Graham Leach Bliley 和数据保护法案等的要求。

威胁防御 VPN—Cisco ASA 5500 系列为远程用户提供了威胁防御接入功能。该解决方案提供了对内部网络系统和服务的站点间访问和远程用户访问。此解决方案结合了对于 SSL 和 IPSec VPN 功能的支持，可实现最高灵活性。因为这一解决方案将防火墙和 Anti-X 服务与 VPN 服务相结合，可确保 VPN 流量不会为医院带来恶意软件或其他威胁。

方便的部署和管理—随此解决方案提供了思科自适应安全设备管理器(ASDM)，它具有一个基于浏览器的、功能强大、易于使用的管理和监控界面。这一解决方案在单一应用中提供了对于所有服务的全面配置。此外，向导可指导用户完成配置的设置，实现迅速部署。

◇ 部署 Cisco IronPort S 系列 Web 安全网关应对来自互联网的 Web 威胁

当前，基于互联网 Web 数据流传播的各种安全威胁，开始在全球范围盛行，使商用网络暴露在这些威胁带来的内在危险之下。现行的网关防御机制已经证明不足以抵御多种基于 Web 的恶意软件入侵。据业内估计，大约 75% 的商用电脑感染了间谍软件，但是在网络周边部署了恶意软件防御系统的企业却不足 10%。基于 Web 的恶意软件传播速度快，变种能力强，其危害性日益严重，对医疗机构特别是网络安全技术相对薄弱的中小型医疗机构来说，拥有一个强健的能够保护医院网络周边并抵御这些安全威胁侵害的安全平台就显得极为重要。

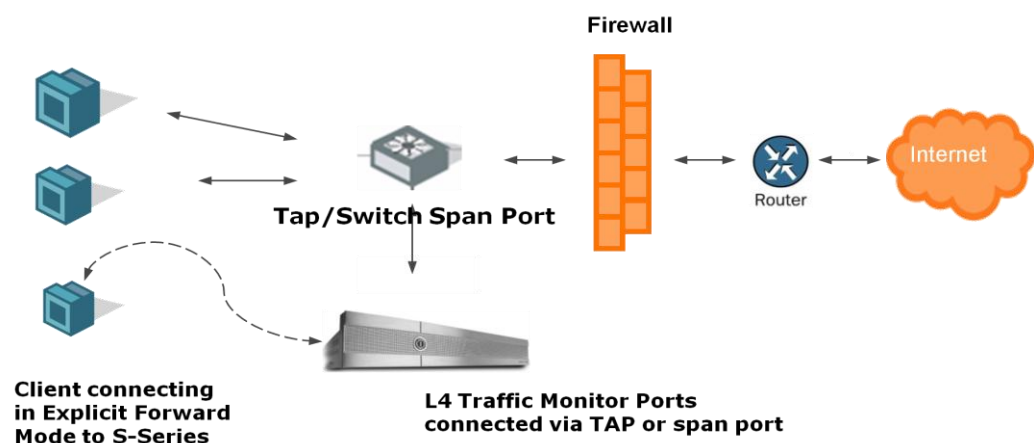
除此以外，当今基于 Web 的威胁 87% 是通过合法的网站发出的。基于 Web 的恶意软件有着速度快、多样性强和变种频繁出现的攻击威胁特点，这要求医院必须使用一个强大的、安全平台才能将日益严峻的上网威胁屏蔽在医院网络之外。

Cisco IronPort S 系列 Web 安全网关是业界开创先河的，也是唯一的将传统的 URL 过滤、信誉过滤和恶意软件过滤功能集中到单一平台来消除上述风险的 Web 安全设备。通过综合利用这些创新的技术，Cisco IronPort S 系列网关能够帮助企业在保证 Web 数据流安全和控制 Web 数据流风险方面，应对所面临的日益严峻的挑战。

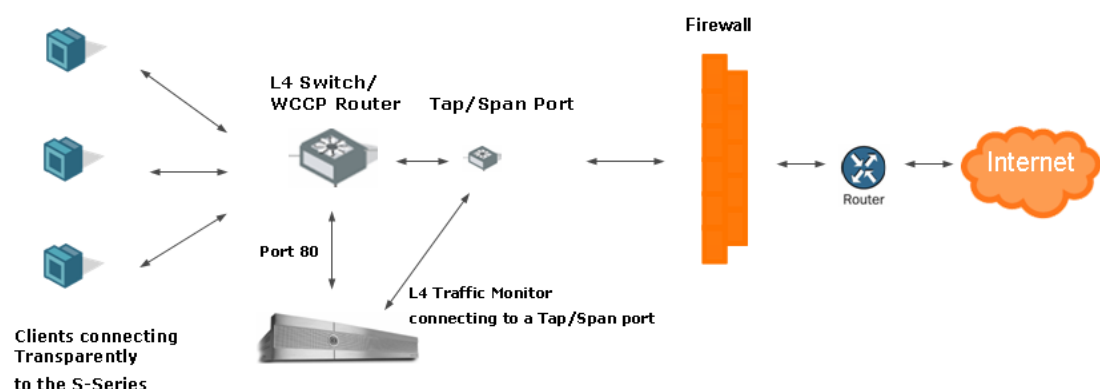
Cisco IronPort S 系列网关结合了多种先进技术，通过单台、集成的网关抵御恶意软件，帮助企业实施安全策略及控制网络流量。提供的多层防护包括 Cisco IronPort Web 名誉过滤器™，多层防恶意软件扫描引擎和第四层(L4)数据流监视器，它可以监控非 80 端口的恶意软件活动。所有这一切为企业提供了一个强大的具有最优性能和功效的 Web 安全平台。同时 Cisco IronPort S 系列提供智能化的 HTTPS 解密的能力，从而对加密数据流应用所有的安全及访问策略。

在实际的应用环境中，医疗机构可以选择以下两种模式部署 S 系列网关：

- 直连模式：客户机直接连接到 S 系列，由 S 系列提供 HTTP/HTTPS/FTP 流量的代理支持。



- 透明模式：由第四层交换机或 WCCP 路由器转发流量至 S 系列，由 S 系列提供对客户机透明的代理支持。



◇ 部署 Cisco IronPort C 系列电子邮件安全网关应对来自互联网电子邮件的安全威胁

垃圾邮件以及随邮件传播的病毒、恶意程序、间谍软件等是当前来自互联网的另一种主要的安全威胁。对于安全技术相对薄弱的中小型医疗机构，这种威胁往往会带来极大的安全风险：随意打开来历不明的电子邮件或者点击邮件中的附件或链接都有可能形成对医疗业务系统的攻击。此外，网络管理人员需要耗费大量精力用于清理垃圾邮件，也严重影响了对正常业务系统的管理和维护。因此，如何对电子邮件应用进行高效的安全防御和管理，也是当前中小型医疗机构部署安全解决方案时需要重点考虑的内容。

Cisco IronPort C 系列电子邮件安全网关是针对电子邮件安全威胁的最佳解决方案。基于 Cisco IronPort 专有的为企业目标设定的 AsyncOS™操作系统，IronPort C 系列能够满足对电子邮件的大容量和高可用性的扫描需求，减少与垃圾邮件、病毒和其他各种威胁相关的系统宕机时间，从而支持对医院邮件系统的高效管理并有效减轻网络管理人员的工作负担。

IronPort C 系列在一个网关设备上集成了思科独有的预防性过滤器和基于特征码的反应性过滤器，配合内容过滤和高级加密技术，为客户提供了目前业界最高级的邮件安全服务。同时，利用思科安全情报运营中心和全球威胁协作组织使 Cisco IronPort 网关产品更聪明，更迅速。这一先进技术使企业可以从最新的互联网威胁中提高他们的安全性，并且使得保护用户更加透明化。

下图描述了 C 系列邮件安全网关的部署方式。



对于中小型医疗机构，本方案涉及的 ASA 和 IronPort 系列主要产品如下表所示：

产品系列	说明
Cisco ASA 5505	提供一体化的安全解决方案，包括防火墙隔离、IPS、VPN、内容过滤等

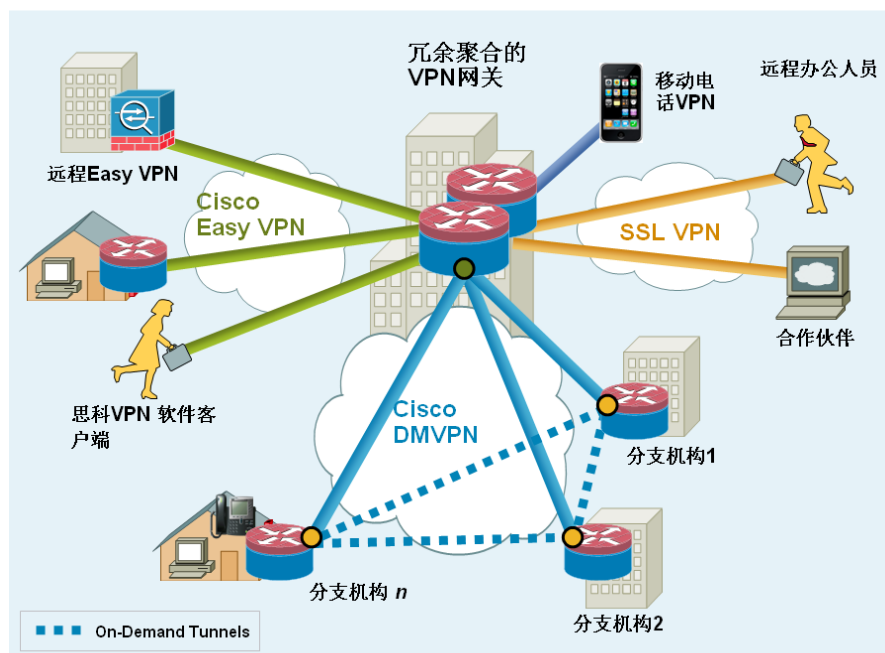
Cisco ASA 5510	提供一体化的安全解决方案，包括防火墙隔离、IPS、VPN、内容过滤等
Cisco IronPort S160	面向中小型医疗机构的 Web 安全网关
Cisco IronPort C160	面向中小型医疗机构的电子邮件安全网关

四、 安全的医疗分支机构解决方案

随着国家不断深化乡镇医疗保障体系的建设，乡镇卫生院、医疗点与城区中心医院之间的联系也日趋紧密。互联网的普及，一方面为这一趋势提供了便利的信息高速公路，但同时也带来了形形色色的安全隐患。在众多的广域网接入技术中，虚拟专网（VPN）可以说是解决这一问题的最具经济实用性的解决方案。

思科基于集成多业务路由器（ISR）的企业级 VPN 解决方案，在可扩展的平台、安全性、服务、应用和管理五大 VPN 实施要素方面，具有基于标准的开放式的体系结构和可扩充的端到端网络互连能力。借助先进的 ISR 路由器，中小型医疗机构用户能够部署多种 VPN 连接方式，通过安全可靠的加密手段，保护医疗应用系统的信息资源。

下图是基于 ISR 路由器的一个典型的 VPN 实施方式：



- 使用思科 ISR 高端路由器 2900 系列做为中心医院的 VPN 网关，用来聚合来自分支医疗机构、合作单位、移动/远程医疗终端的 VPN 各种应用。
- 在分支医疗机构中，根据机构的规模和应用状况可选择思科 ISR 路由器中的 1900 系列、890c 系列或 880c 系列做为 VPN 的网关。

方案特点：

1. 安全保障

虽然实现 VPN 的技术和方式很多，但所有的 VPN 均应保证通过公用网络平台传输数据的专用性和安全性。在安全性方面，由于 VPN 直接构建在公用网上，实现简单、方便、灵活，但同时其安全问题也更为突出。医院必须确保其 VPN 上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问。

2. 服务质量保证 (QoS)

VPN 网应当为医院数据提供不同等级的服务质量保证。不同的用户和业务对服务质量保证的要求差别较大。在网络优化方面，构建 VPN 的另一重要需求是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，使实时性要求高的数据得不到及时发送；而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略，可以按照优先级分实现带宽管理，使得各类数据能够被合理地先后发送，并预防阻塞的发生。

3. 可扩充性和灵活性

VPN 必须能够支持通过 Intranet 和 Extranet 的任何类型的数据流，方便增加新的节点，支持多种类型的传输媒介，可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

4. 可管理性

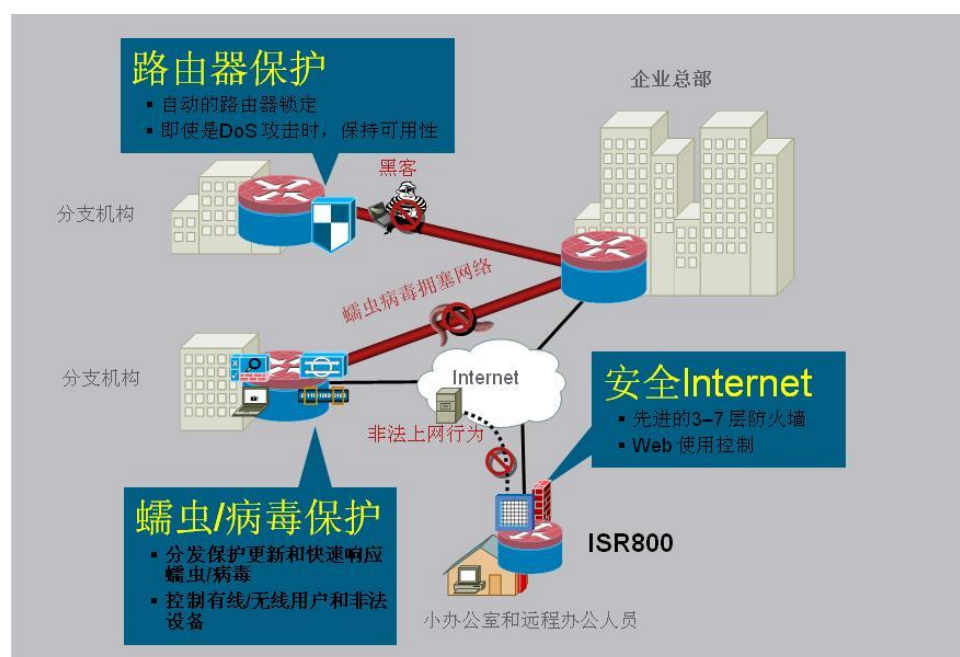
从用户角度和运营商角度应可方便地进行管理、维护。VPN 管理的目标为：减小网络风险、具有高扩展性、经济性、高可靠性等优点。事实上，VPN 管理主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS 管理等内容。

5. 多种 VPN 的连接方式

思科公司基于 ISR 路由器 VPN 解决方案为中小型医院用户提供了多种 VPN 的连接方式，包括 IPSec、SSL、动态多点 VPN (DMVPN) 等。

与中心医院通常有较为完善的网络安全部署不同,对于大量的分支医疗机构,如乡镇卫生院、医疗服务点等,如何部署合适的网络连接设备应对当前的各种网络威胁,例如:黑客攻击,蠕虫病毒,非法上网行为等等,是另外一个需要考虑的重要问题。这些网络威胁,既冲击了分支医疗机构的网络安全,又消耗了大量网络资源,严重影响了医疗系统的正常运行。

思科新一代的ISR800系列路由器为中小型的分支机构和小型办公室提供了可靠的网络解决方案,来防御各种网络中的威胁,保证了网络资源应用,确保了医疗机构广域网络的正常运行。



- 思科 ISR 路由器部署在分支机构, 提供了安全的 Internet 访问
- 提供先进的防火墙, 能够监控电子邮件, 即时消息传递和 HTTP 流量
- 可以在分支机构的本地设备实施防御蠕虫病毒的安全策略, 节省广域网络带宽
- 入侵防御系统 (IPS): 这种深度包检测特性能够有效阻止各种网络攻击
- 内容过滤: 一种基于预订的集成安全解决方案, 能够提供基于类别的分级; 关键字拦截; 并可抵御广告软件、恶意软件、间谍软件和 URL 拦截
- 即使是 DOS 攻击, 也可保持可用性

方案中涉及的主要 ISR 路由器产品:

产品系列	说明
Cisco2921	部署在中心医院
Cisco1941	部署在较大规模的分支机构，例如分院
Cisco860/880C/890C	部署在卫生院、医疗服务站等

此外，思科还提供精睿系列 VPN 路由器，专为需要基本远程安全互连且严格控制投资预算的小型医疗分支机构提供入门级的 IPSec VPN 连接，并且可以与中心医疗机构的思科 ISR 路由器统一部署，提供一体化的 VPN 解决方案。常用的精睿系列 VPN 路由器如下：

产品系列	说明
Cisco RV120W	部署在小型分支机构，支持 10 个 IPSec 隧道和 802.11n
Cisco WRV210	部署在小型分支机构，支持 5 个 IPSec 隧道和 802.11g
Cisco RVS4000	部署在小型分支机构，支持 5 个 IPSec 隧道和 IPS

五、 医院网络安全管理解决方案

随着医院网络建设的深入，安全产品不断增加，整体缺乏统一管理，相互间没有沟通交互，信息无法有效整合，是一些信息安全的孤岛。就象现在人们在关注和谈论的 IT 孤岛问题一样，各个应用系统之间缺乏有效联系，信息得不到整合，发挥不出其应有的价值。同样的问题放在网络安全上，这一效应就有可能放大成为风险，给企业 IT 系统的持续运转埋下隐患。

思科安全管理器（Cisco Security Manager, CSM）是思科安全管理套件的一部分，能够为思科自防御网络全面管理并执行各种策略。与无法协同运行、存在很多漏洞的多家厂商提供的单点安全产品不同，该套件提供了一个全面的配置、监控、移植和身份识别解决方案，能够有效提高网络的安全性、永续性和易操作性。它可充分利用医院现有的网络和安全投资，来识别、隔离被攻击的组件和建

议对其精确删除的方式。它也有助于保持医院内部策略符合性，可作为整体法规符合性解决方案工具中一个不可缺少的部件。

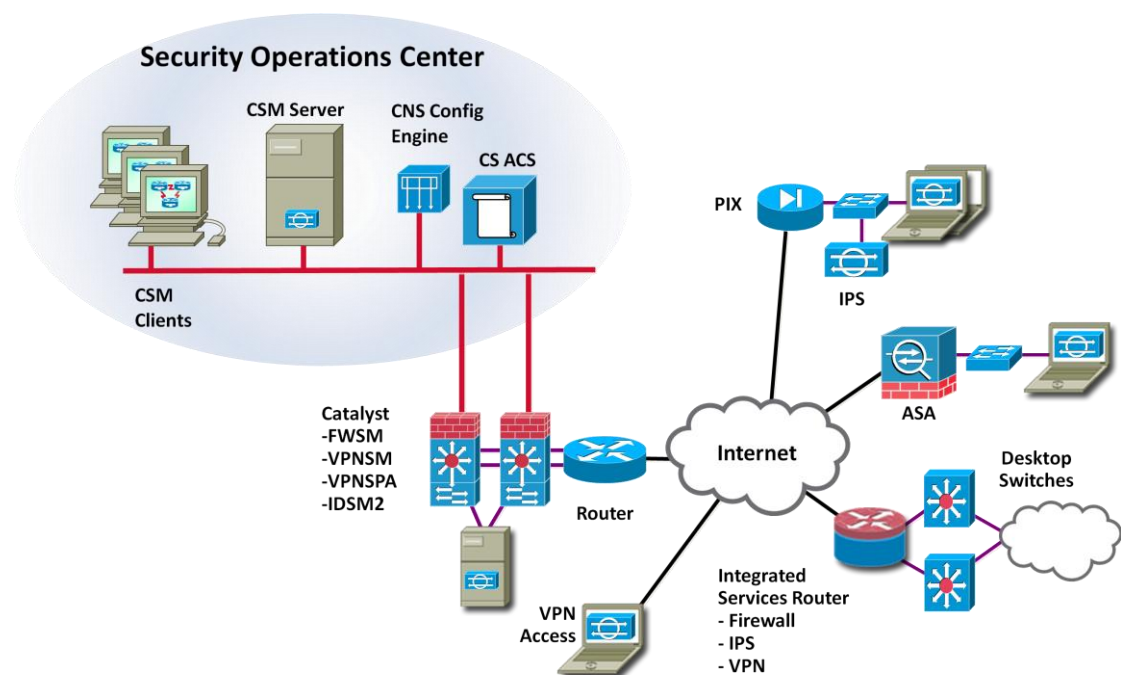
医院安全和网络管理员所面临的问题有：

- 安全和网络信息过载
- 性能不佳的攻击和故障识别、优先级划分和响应
- 更高攻击先进程度、速度和修复成本
- 满足法规符合性和审查要求
- 较少的安全人员和预算

思科 CSM 可通过以下功能满足其需要：

- 集成网络智能，进行网络异常事件和安全事件的先进关联
- 察看校正后的事件并自动执行调查
- 通过全面充分利用网络和安全基础设施来防御攻击
- 监控系统、网络和安全运行来帮助医院达到法规符合性
- 以最低 TCO 提供一个易于部署和使用的、可扩展的设备
- 将网络安全设备大量的告警信息进行综合整理归纳使其具有可读性

下图为 CSM 的部署方式：



思科安全管理器采用了基于策略的强大管理技术，能有效管理各种规模的网

络，而它功能丰富的客户端图形用户界面则提供了出色的易用性。为完成不同的任务，满足用户的不同要求，思科安全管理器提供多种应用视图，例如图 1 所示的以设备为中心的视图，以及图 2 所示的以地图为中心的视图。

图 1 以设备为中心的视图提供了一个简化界面，用于添加设备以及编辑和部署安全策略

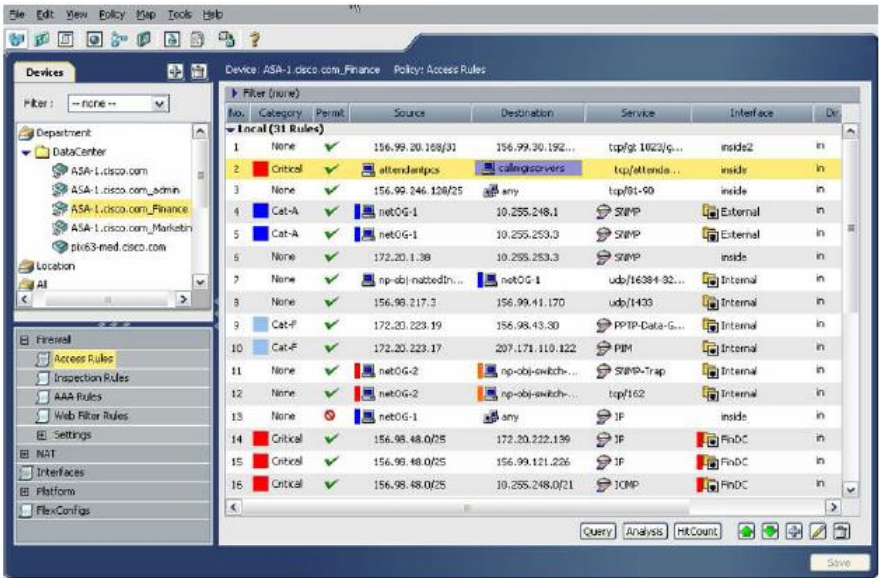


图 2 以地图为中心的视图使用户能以可视方式管理策略和设备



六、 思科网络安全解决方案优势

计算机网络不仅仅要具有保护网上主机系统，网上终端系统，网上应用系统的能力，关键是要网络本身也具有自我保护能力，自我防御能力，自我愈合能力，做到即保护网络应用的同时，又保护了网络自身。而这正是思科所倡导的“自防御网络”计划。思科自防御网络计划是一种多阶段安全计划，大大提高了网络发现、预防和对安全威胁的能力。适应未来信息系统发展的要求。思科为采用传统和新兴技术的综合应用环境提供了一个具高度永续性、响应能力和可扩展性的解决方案。

网络威胁防御不是单独的设备添加，而是一个系统。安全已经变成了网络的一部分，已经和网络密不可分，安全无处不在。思科的网络安全解决方案包含了威胁防御、安全通信、安全的网络服务以及全方位的安全管理。涉及到网络安全的方方面面，融合了有线及无线网络，提供统一的安全策略。提供了业界最完整的安全解决方案，为整个医院业务应用的稳定运行保驾护航。

思科不仅仅可提供安全的解决方案或设备，同时可提供专业的安全服务，对整个系统进行安全评估，提出解决方案。并可针对医院业务应用需求提出网络安全设计策略。

详细信息欢迎垂询思科区域中小企业客户经理和中小企业客户技术支持工程师，或参考思科网站：

- **English:** www.cisco.com
- **中文:** www.cisco.com.cn

第五章 中小型医院无线网络及应用解决方案

一、 中小型医院的无线需求

对于一个现代化的医院来讲。如何能快速、及时地把病人数据传输到医生那里用于诊断,减少与降低患者的就医时间和成本?如何使医护人员的查房提高工作效率并可避免因字迹模糊潦草而导致医疗事故的发生?这些都是医院管理者需要重点考虑的问题。

近几年,随着国内医疗体制的改革与医药分离的出现,医院之间也形成了竞争格局,它不仅仅体现在医院医疗水平的高低,同样也体现在医院所具备的医疗设备以及对患者的服务质量方面。在计算机技术高速发展的今天,国内大部分医院都采用了 HIS 医院信息管理系统来提高医院的工作效率与服务质量。但不少医院的信息系统化在很大程度上只是医院管理流程的计算机化,并不是真正的医疗信息化。现代医疗信息化的核心是病人信息的共享,包括医院各个科室之间比如化验科、放射科、造影室与医生之间的即时信息共享,甚至是医院之间、医院与社区之间的信息共享,以数据库为中心实现病人信息的无纸化和无胶片化,这就需要强大的网络支持。此外,由于医疗行业的特殊性,医护人员和病患者之间需要频繁地在院内移动、同时处理大量的信息,这些都要求网络具备可移动性、传输速率高等特点。同时考虑到医院业务量的增加,网络需要留出足够余地扩容而不影响医院正常的工作。这些显然已不是传统网络所能满足。

伴随着 IEEE802.11 系列无线局域网(WLAN)标准的出现及无线技术的大力发展,芯片、终端等整个产业链全面支持无线技术,使“网络无处不在”的美好愿望成为现实,同时其具备的移动性和灵活性,使得医院部署特殊的信息化应用成为可能。Cisco 针对目前国内大多数中小型医院的需求制定了无线医疗网络解决方案,帮助医疗人员大大节省时间、提高工作效率和工作准确度,实现改进工作流程、完善管理考核的目的。

二、 中小型医院的无线应用

医疗行业的无线应用非常丰富,如药库中种类繁多的药品通过基于无线应用的条码扫描枪可以大大提高库房管理的效率;如通过无线 RFID 标签的使用,可以实现人员和贵重设备的追踪、定位功能等等。思科公司根据中小型医院的特点,从投入成本及应用普及度考虑,推出适合于中小型医院部署的相关无线应用解决方案。

1. 护士呼叫系统

通过无线 IP 电话的应用，可以将传统的护士呼叫只能到护士站的方式，改进为护士站和护士随身携带的无线 IP 电话同时振铃，或者改进为当护士站没有人接听后再转接到护士的无线 IP 电话上。护士可以看到呼叫者的病床号、能够接听处理，如果在一定的时间内没有接听，系统将向预先定义的上级人员发出通知信息。通过该系统，既可以提高病患的满意度，又可以详细记录工作情况，提高管理透明度。护士呼叫系统的详细说明参见高效协作部分。



2. 无线上网

无线网络除了处理医疗应用外，还可以为病人和医护人员提供方便的 Internet 网络连接。尤其是在医院有限布线点不足的问题，通过采用无线网络的方式解决，更加游刃有余。

医院的有线网络，一般分为内网和外网。但是无线技术本身的限制，使同一区域没法实现部署两套独立的网络。所以在同一区域，内网和外网只能是同一个无线网络。此时，如何保证内网的医疗应用安全、以及外网 Internet 服务的顺利进行，就非常重要了。

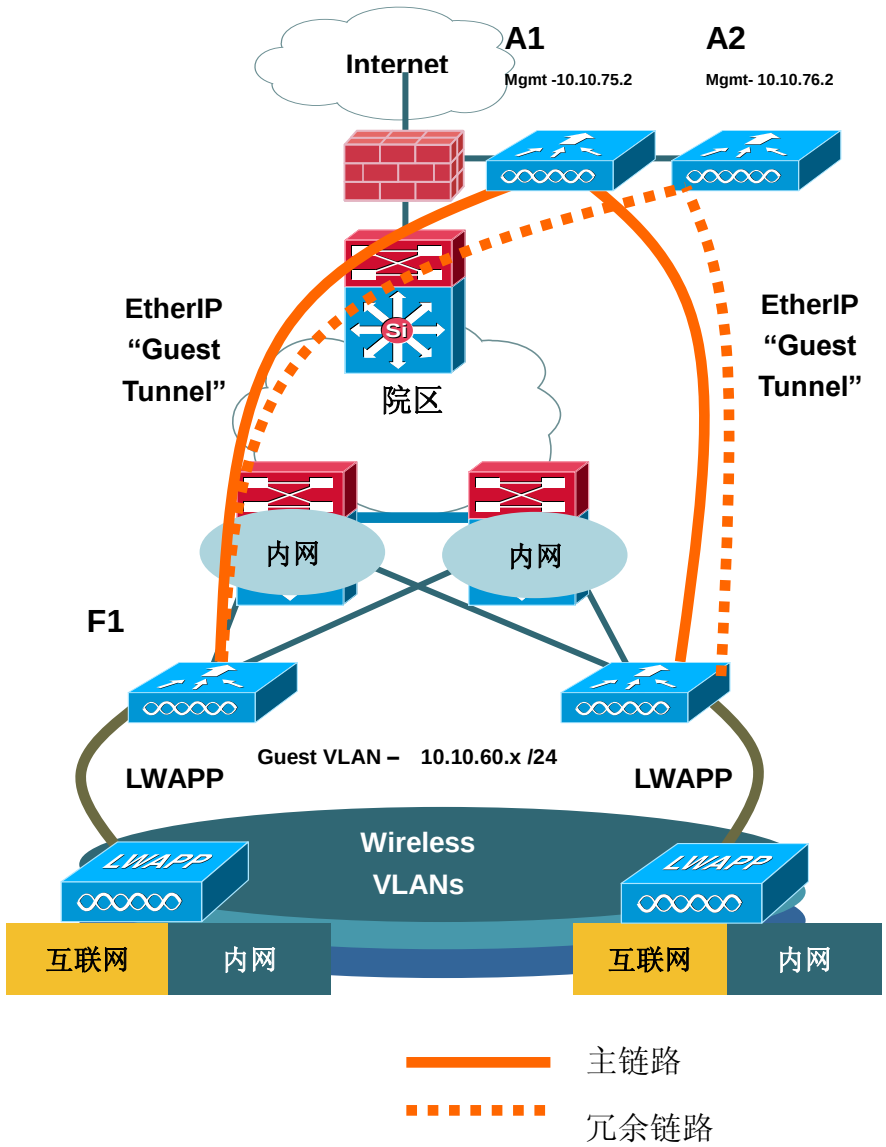
通过思科访客隔离接入解决方案我们一方面要为内网的用户提供高级别的安全认证（支持多种认证方式）和数据加密；另一方面，要为外网的用户提供简单易用的认证方式，而且，最好把互联网的数据流，直接送到外网的防火墙上，从而避免对内网数据的访问。

由于无线网络的技术限制，同一个区域无法部署内网和外网两套不同的网络。思科独有的无线访客技术可以保证病人等无线外部用户与医院等内部用户的隔离。将外部用户逻辑隔离，在允许外部用户访问互联网的同时保证内部无线用户的安全。

如下图所示方法，互联网用户采用独立 VLAN，在防火墙的非军事化区配置

独立无线控制器，所有互联网的流量通过 Tunnel 终结在非军事化区。还可以通过备份链路实现冗余。另外，网管软件或控制器自带的 Lobby 管理员功能，可以为 Lobby 用户提供简单的界面，建立用户，并生成用户的密码，用户的有效期。

Lobby 管理员界面简单、功能明确，非常适合病房等使用。例如：护士台可以通过简单明确的界面给病人或家属设置一定有效期的用户名、口令。



(图) 思科访客隔离接入解决方案

三、 思科无线解决方案优势

面对医疗行业丰富的无线应用需求，思科无线网络不仅可以满足各类应用需求，还可以全面解决医院无线网络部署时的各种顾虑。

思科的无线解决方案包括自治型 AP 方案和集中式轻型 AP 方案，俗称“胖”AP 方案和“瘦”AP 方案。所谓“胖”AP 方案，是指每个 AP 都是独立设备，需独立配置、独立工作，实现无缝漫游时技术复杂；所谓“瘦”AP 方案，是指每个 AP 完全不需配置，全部的配置和管理都通过中心控制器统一实现。由于 AP 全部注册在控制器上，控制器可以对所有管理下的 AP 的无线射频实现实时动态的调整，从而实现更好的无线覆盖和更智能的流量负载均衡；而且无缝漫游、无线定位的实现非常简单。为实现部署的灵活性和投资保护，思科的两种无线 AP 可以自由转换，即通过 AP 的软件更换，AP 可以工作在胖 AP 模式，或者瘦 AP 模式。当然在瘦 AP 模式时，基本方案除了 AP 外，还需要添加无线控制器。

思科无线“胖”AP 方案，包括无线 AP 及其天线，可选配无线网管软件；无线“瘦”AP 方案，包括无线 AP 及其天线、无线控制器 WLC。可选配无线网管软件 WCS 以支持更多丰富的管理功能。如果需要使用定位功能，还可以选配思科无线定位服务器 MSE。

思科的无线解决方案全面支持 802.11a/b/g/n 技术标准，还支持先进的无线射频动态调整、网络负载自动均衡、快速安全的移动漫游等功能，另外，在无线网络安全、访客隔离、远程无线部署、无线语音支持、方便的无线管理等方面技术领先。

“胖”AP 架构成本低一些，但是大规模部署时，管理、运行、维护的成本高；“瘦”AP 架构成本高一些，但是管理、运行、维护的成本低，而且易于漫游、易于定位。思科抽取国内二十家使用思科无线网络的医院统计结果表明，平均每家医院的 AP 数量在 100 个左右，因此医院适合于采用“瘦 AP”的架构，建议 AP 能够实现“胖”“瘦”的自由转换，以提高灵活性、保护用户投资。

1. 无线射频智能频谱管理功能

由于 Wi-Fi 在共享无需授权的波段工作，因此，要在 Wi-Fi 网络中支持高级别性能、安全性和可靠性，必须拥有集成式频谱智能和频谱管理。频谱管理对于在关键无线应用中为最终用户提供丰富、可靠的移动性体验至关重要。

商用 Wi-Fi 芯片集的有限射频可见性功能不能满足需要，因此思科集成了获得专利的频谱处理硬件和软件，专用于分析干扰，而且还创建了真正的企业级 Wi-Fi 芯片集。由于具有这种底层硅片功能，Cisco CleanAir 技术可对各个干扰源进行分类，并找出干扰源，告诉您它们如何影响网络性能或安全性。

Cisco CleanAir 是一种革命性的技术，在业界尚属首例。使用该技术，IT 经理可以访问自动收集的关于每个非 802.11 干扰源的丰富频谱信息。CleanAir 技术提供的频谱智能支持全新级别的频谱管理。与以前的频谱管理工具相比，新的集成式频谱管理是无线网络结构的一部分，而以前的频谱管理工具则仅适应于

其他 Wi-Fi 设备，并且通常与无线网络分离。第二代频谱管理可充分感知所有无线频谱用户，而且能够采取行动来缓解或避免干扰，从而优化网络性能。

CleanAir 技术广泛应用于思科统一无线网络系统内部，通过以下方式提高无线质量：

- 侦测其他系统无法看到的 射频 干扰
- 识别来源，并在平面图中找到相应的位置
- 自动调整以优化干扰周围的无线覆盖范围

这一创新技术的优势在于：

- 自我修复和自我优化无线网络
- 更快地排除故障，减少中断时间
- 有效地实施策略
- 提供物理层安全性

2. 无线网络安全功能

思科提供了基于有线无线集成的统一的端到端的安全架构。思科无线网络的解决方案支持高效、多级别、多种类、多级的认证方式和加密技术，具体如下：

- **无线终端用户的用户认证（用户名/密码，数字证书）、无线终端用户的数据加密(WEP, TKIP, AES)** —思科无线网络系统在使用 802.1X-EAP、TKIP 或 AES 时，可以防止网络遭受多种网络攻击的影响
- **无线接入点的接入认证** —通过 X.509 证书、AP 的 802.1x 认证，保证合法的 AP 才能连接到无线网络中；
- **无线控制帧的安全管理 (MFP)** —管理帧保护功能能够很好地保护无线客户端与无线 AP 之间的 802.11 管理帧，防范针对管理帧的无线攻击，避免无线客户端和合法 AP 之间总是断开；
- **无线 IDS 以及无线和有线 IDS/IPS 联动功能** —思科无线网络自带 L2 WIDS 功能，通过和有线网络的 IDS/IPS 联动，可以实现对 L2-L7 入侵攻击的防范，实现有线网络和无线网络的一体化，实现一体化的最大安全性
- **基于 2-7 层内容的入侵检测系统（无线 IPS、IDS 系统）**
- **支持精确的非法 AP 定位和隔离** —保证无线网络免受无线类的安全攻击

- **终端的安全接入保证 (NAC)** — 无线用户接入到网络中时，对用户终端的操作系统版本、补丁情况、病毒库版本进行检查，以确保系统的安全性。这样即使拥有了合法的用户名和密码或者安装了合法的数字证书，也只有满足系统要求的终端才能连接到网络中，从而大大提高整个网络系统的安全性。
- **终端快速、安全漫游机制的实现 (CCKM)** — 对于高安全级别的医疗应用，建议数据进行加密。在漫游过程中，数据的加密密钥需要交换，思科通过 CCKM 机制 (Cisco Centralized Key Management) 来保证高速、高效的安全切换，通过这种方式，可以加速密钥交换过程，从而缩短切换时间，从而保证业务的顺利进行。
- 独特的外部用户隔离机制—详见后文。

医院在使用无线网络时，解决好以下的安全的问题是非常重要的：

- 必须能够防止非授权人员使用医院无线网络
 - 解决方法：通过思科无线网络和思科 AAA 软件：Cisco Secure ACS，实现用户名和密码认证，支持多种认证和高级加密方式
- 避免医护人员每次开机输入用户名和密码的麻烦
 - 解决方法：将用户名和密码缓存
- 防止非授权终端使用医院无线网络
 - 解决方法：用 ACS 进行终端 MAC 地址的集中认证和管理；或通过高级的用户名/口令认证
- 保证数据的私密性和完整性
 - 解决方法：采用 WPA2 或 WPA 代替 WEP，采用 AES 加密；
- 攻击源查找
 - 解决方法：能够检测非法 AP，并压制和定位；能够接合有线网络的 IPS 系统，实现主动防御的安全管理

3. 思科独特的访客隔离接入解决方案

4. 思科 ClientLink 波束成形技术

在未来几年 Wi-Fi 网络将过渡到 802.11n 技术。在此期间，无线网络将要支持 802.11a/g 老客户端和 802.11n 客户端混合的环境，特别是医疗行业所需要的各类手持终端只支持 802.11a/g 的技术。因为 802.11a/g 老客户端工作在较低的数据传输速率，老的客户端将拖累整个网络，降低网络的性能。 ClientLink

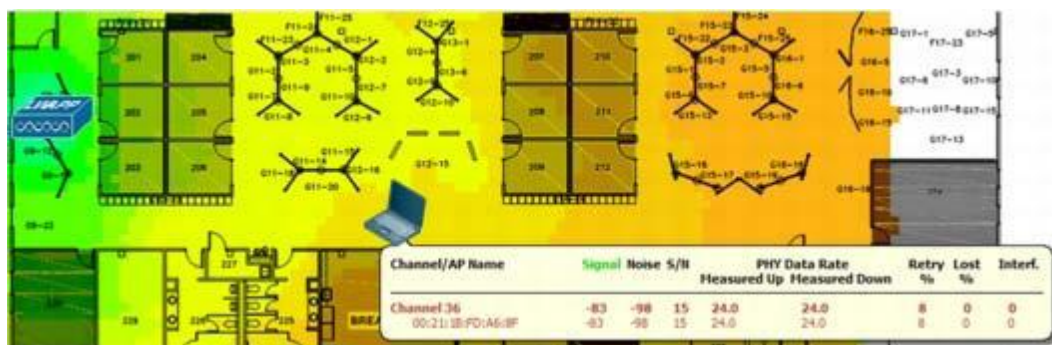
波束成形技术（以下称为“ClientLink 技术”）可以帮助解决在混合客户端的 802.11n 网络下带来的有关的问题，使用户确信即便是当 802.11a/g 客户端靠近信号覆盖的边界时也可以以最佳的速率运行。

在混合的环境中，老的 802.11a/g 客户端将增加 802.11n 客户的通讯时延，从而降低网络的性能。思科认识到要为企业保护他们在这些的 802.11a/g 设备上的投资的需求，为此，思科已经开发出一种新技术，使企业 802.11a/g 的客户端设备也能够从部署 802.11n 带来的性能优势中受益，从而延长其使用寿命。

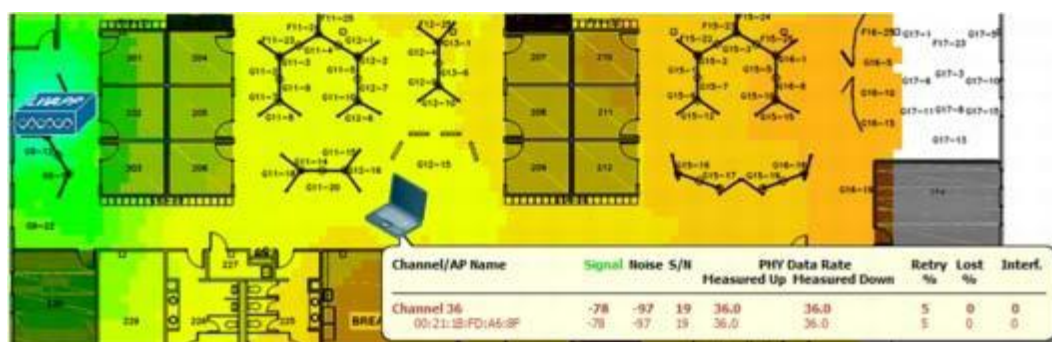
大多数的 802.11n 解决方案是改进提升客户端到无线接入点间的上行通信速率。思科 ClientLink 技术之所以是业界唯一的，因为它不仅提升了客户端到无线接入点间的上行通信速率而且也提升了下行通信速率。这一点很重要，因为局域网中日常大多数的通讯，如 Web 浏览，电子邮件和文件下载是发生在下行方向。提升最慢的客户端的下行链路吞吐量，提升的不仅仅是慢的客户端的无线网络使用体验，而是提升无线网络中全网用户端的无线网络使用体验。ClientLink 技术使用的结果将是为用户提供更加稳定可靠的漫游经验并提升全网的性能。思科公司在 Wi-Fi 芯片组内增加了先进的信号处理模块。多发射天线被用来针对 802.11a/g 客户端集中传输的方向进行优化，以提高相同覆盖信号范围内的下行信噪比和数据传输速率，从而减少信号覆盖盲区并提升整体网络系统性能。这种技术的基本原理是采用学习的方式，结合最优化的方法，分析接收到的客户端的信号，然后以最优的方式将数据返回给客户端。这种技术也被称为 MIMO（多输入多输出）波束成形，传输波束形成，或同相位技术，它是在市场上唯一的、不需要额外通过昂贵的天线阵列来实现的企业级解决方案。

思科 ClientLink 技术可以让无线接入点有效地优化客户端所在位置的无线信号的信噪比。优化信噪比带来许多好处，如降低重传次数和建立更高的数据速率。例如，以前一个在信号覆盖边缘的客户端以 12 Mbps 数据速率接受数据包，而现在可以达到 36 Mbps。在典型的下行性能测试中采用 ClientLink 技术，802.11a/g 客户端下行通信方向的吞吐量性能可以提高 25%。ClientLink 技术可以让 Wi-Fi 系统以更少的重传和高数据速率的方式工作，提高了整体网络系统的性能，这意味着最有效地使用频谱资源。

无线网络中，在许多信号覆盖边缘的区域通常存在一些覆盖盲区，在这些盲区内由于信号太弱而影响 Wi-Fi 网络的性能。当客户端在无线接入点覆盖区域之间漫游时，经常会面临覆盖盲区的问题。思科 ClientLink 波束成形技术可以减少信号覆盖的盲区和提高信号覆盖的范围，确保无线信号更可靠，可预测，且均匀覆盖整个楼面。如下图证明了采用 ClientLink 技术，客户端如何获得的最高数据传输率。在这一特定的示例中，信号强度提高了 5 分贝，数据传输速率从 24 Mbps 提高到 36 Mbps。



没有采用 ClientLink 技术时的信号覆盖热图



采用 ClientLink 技术时的信号覆盖热图

5. 无线语音支持：

在医疗的无线应用中，可以看到未来无线 IP 话机的应用将越来越多。作为无线平台的部署，必须要具备支持无线语音应用的能力。

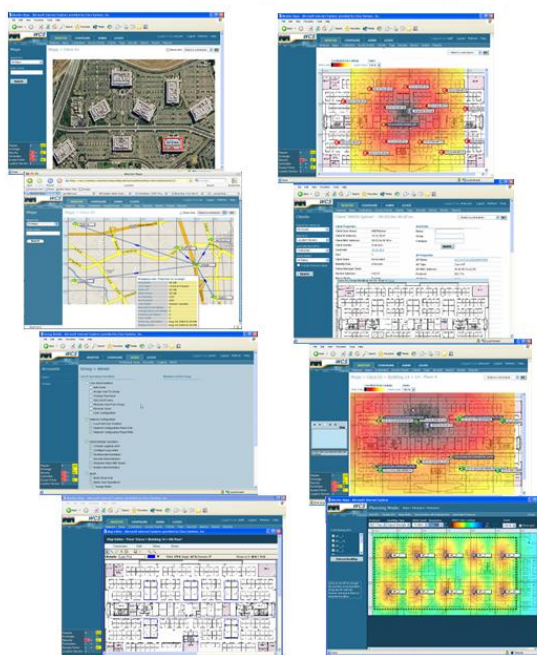
无线语音应用不仅要保证足够的带宽、低网络延迟、等 QoS 特性，还需要实现其它功能，如：

- **基于无线系统的节电功能** —通过 U-APSD 的功能，使无线终端，特别是语音终端的电池使用时间对比没有使用该功能以前增加 2-4 倍
- **基于无线系统的动态功率控制 DTPC** —通过动态功率控制 DTPC (Dynamic Transmit Power Control)，无线 AP 可以自动通知无线客户端互相协商其发射功率，避免单通问题，同时还可帮助客户端进行节电
- **基于无线系统的呼叫控制** —对于 WLAN 网络里的无线 AP 来说，能接入客户端的容量并不是无限的，当大量无线客户端同时接入同一个 AP 的场景，会对一个 AP 的处理能力产生一个瓶颈。那么，在超过一个 AP 的语音接入容量的情况下，如果没有控制策略，会造成每路语音的通话质量全部下降。如果能提供呼叫控制，则可避免该情况。而呼叫控制可以基于语音流量进行，也可基于无线信道负载进行。

- **VoWLAN 的快速漫游机制** —通过 CCKM 机制 (Cisco Centralized Key Management) 来保证语音应用的快速安全漫游。

6. 易于管理

网络管理 - 思科无线控制系统 (WCS)



世界级网络管理

特性:

- 计划、配置、监控、位置、IDS 和故障修复
- 分级管理
- 直观的图形用户接口和模板
- 网络策略(QoS、安全、RRM等)

优点:

- 更低的 OPEX and CAPEX
- 更好的空间可见度和可控度
- 功能增强的单管理系统

思科无线网络管理系统 (WCS) 提供了快速有效的方法来对采用思科无线网络产品构建的网络进行管理和故障排除。这一功能强大的应用提供了全套网络可视化、发现、故障和诊断能力, 以在其影响网络服务之前识别问题。

WCS 包含射频建模软件, 可根据输入楼层的情况自动确定接入点位置来帮助自动决定接入点的初始布局。WCS 可以输入站点勘察工具的勘察结果, 并进行优化, 使得部署 WLAN 的工作能够非常顺利地进行。(当然, 不管使用什么工具, 仍然需要手工进行站点勘察, 这是勘察工具所不能代替的。)

像思科的 WCS 规划工具可以在基于 CAD 的楼层规划中对诸如混凝土外墙和金属门之类的建筑物指定预设衰减级别, 确定接入点位置、信道分配、功率输出设置以及其它配置属性。它们使用用户密度和吞吐量这类参数作为标准。在接入点勘察工作完成后, 还可以验证和描述这些接入点的覆盖区域。

管理员可以用 WLAN 管理软件系统来完成所有长期管理和优化工作。该工具与 RF 扫描并用, 能够检测和查找欺诈设备和人员, 使用 WLAN 管理软件系统将最新发现的设备显示在平面图上。管理员还可以将 WLAN 管理软件系统用于用户管理。该工具能够在平面图上找到用户, 显示用户的网络使用统计数据、漫游历史和地址细节。

另外，无线网管软件 WCS 还支持客户端故障排查：

- 帮助网络维护人员远程诊断、排除客户端问题
- 通过提示步骤逐步调试 1 到 3 层的客户端问题
- 标注不同网络层问题
- 系统主动分析深层的细节与日志
- 提出修正方法

四、 思科无线解决方案设备参考

- 无线接入点 AP（LAP 与 AP 可以胖瘦灵活转换）
 - LAP / AP：1141/1142（802.11a/b/g/n，内置天线）
 - LAP / AP：1042（802.11a/b/g/n，内置天线）
 - LAP / AP：1252（802.11a/b/g/n，外接天线）
 - LAP / AP：1262（802.11a/b/g/n，外接天线）
 - CAP：3500i(802.11a/b/g/n，内接天线，支持 CleanAir 技术)
 - CAP：3500e(802.11a/b/g/n，外接天线，支持 CleanAir 技术)
- 无线控制器 WLC（可以冗余配置、可以集群管理）
 - NME-AIR-WLC6-K9（ISR 无线控制器模块：支持 6 个 AP）
 - NME-AIR-WLC8-K9（ISR 无线控制器模块：支持 8 个 AP）
 - NME-AIR-WLC12-K9（ISR 无线控制器模块：支持 12 个 AP）
 - NME-AIR-WLC25-K9（ISR 无线控制器模块：支持 25 个 AP）
 - AIR-WLC5508-X-K9（独立的无线控制器 5508：分别支持 12,25,50,100,250,500 个 AP，并可通过购买 License 升级支持的 AP 数量）
- 安全认证与管理服务器（可以冗余配置）
 - CSACS-5.0-EXP-K9（Cisco Secure ACS Express：软件）
 - CSACS-1120-K9（Cisco Secure ACS：软硬件一体）
- 无线网络管理（根据 AP 数量选择）
 - WCS-APBASE-50（50 个 AP 的无线网管）

- WCS-APBASE-100 (100 个 AP 的无线网管)
- 无线定位服务器
 - AIR-MSE-33xx-K9 及相应 License

详细信息欢迎垂询思科区域中小企业客户经理和中小企业客户技术支持工程师，或参考思科网站：

- **English: www.cisco.com**
- **中文: www.cisco.com.cn**

第六章 中小型医院高效协作解决方案

门诊是医院的主要窗口，是为病人提供优质服务的界面，人员流动量大，病种繁多，对象复杂，诊治各种手续繁多，如何能够解决病人就诊排队无序、医生工作量不平衡、环境的嘈杂等问题是急需考虑的问题。住院部是医院收住患者，病理观察及手术恢复的场所，需要为患者提供全方位的护理服务，如何能够及时、准确、快速的对患者所需要的帮助做出响应，同样也是医院管理者需要重点考虑的问题。

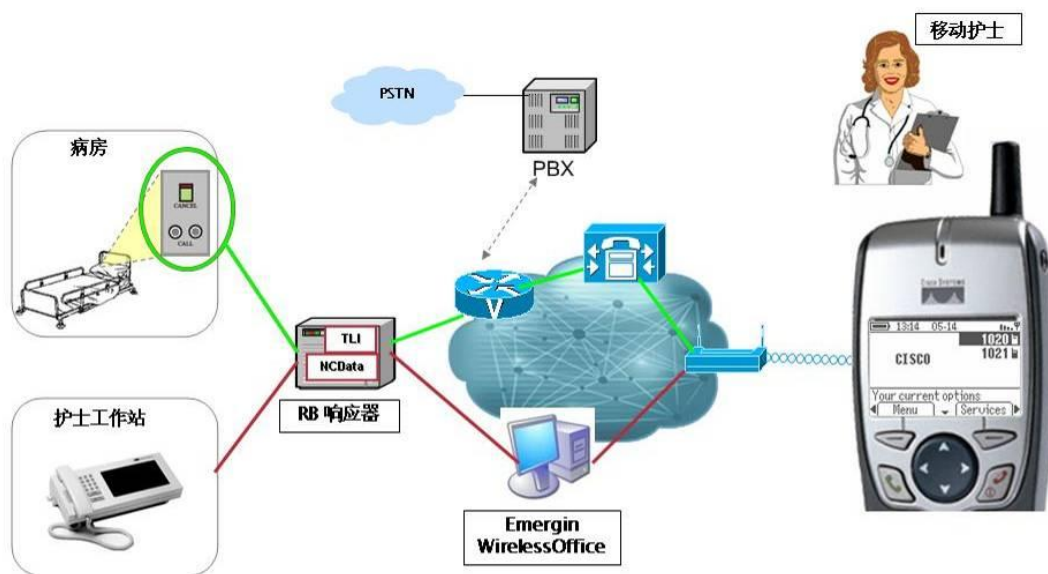
中小型医院通信的目标，是如何充分运用方便的通信沟通手段，提高患者满意度，提高医护人员的工作效率，有效地跨部门协作，实现医疗导诊、护士护理服务、远程会诊，提高诊断的正确性，这就是思科协作解决方案在中小型医院通信系统中的价值所在。下文中将详细介绍思科在中小型医院协作通信上的几个应用方案及相关设备。

一、 中小型医院协作应用

1. 护士呼叫系统

传统的护士呼叫系统是当某个患者按下床边按钮寻求帮助时，护士办公桌上的一盏灯就会立即亮起。负责监控的人员通常就会使用嘈杂的顶置寻呼系统要求某位护士前往该病房。这个过程非常缓慢、低效，而且会对其他患者产生影响。

思科护士呼叫系统解决方是当患者按下床边按钮时，一个文本消息会被直接发送给负责该病房的护士。护士不再需要立即停止她们正在处理的工作。她们可以拿起电话，查看消息，她们也可以立即致电医生，要求进行进一步的药物治疗。这样，问题可以迅速地得到解决。利用它，来自病人的呼叫也可以直接被接驳到护士手上的无线 IP 电话上，护士可以第一时间知道病人的情况。另外，该护士呼叫系统还可以减少错误警报引起的时间浪费。利用新的护士呼叫系统解决方案，护士完全可以根据病人的病情给予最适当的护理。



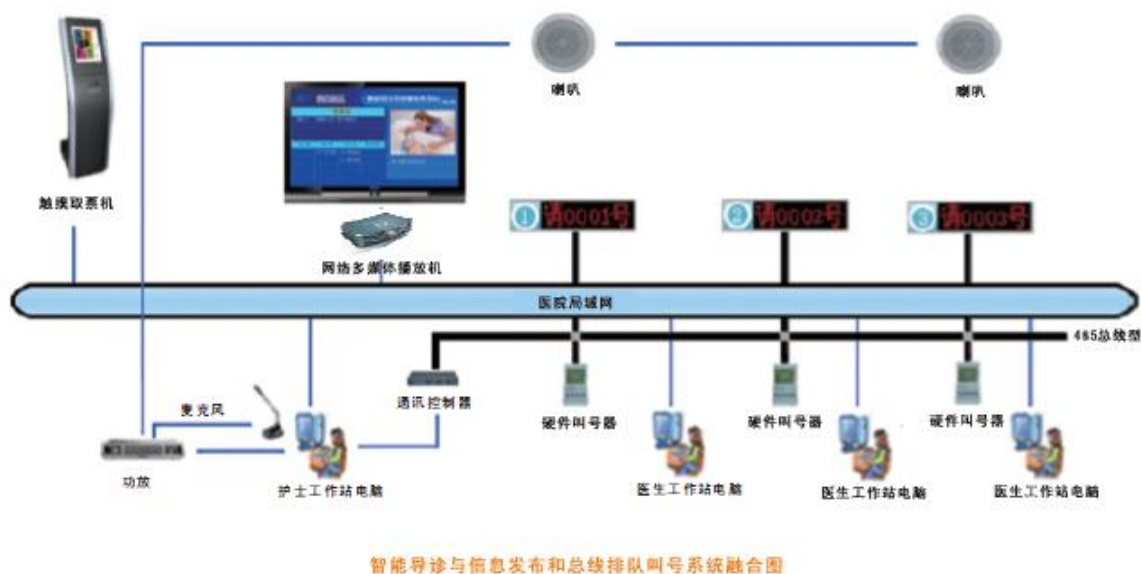
(图) 护士呼叫系统

那么，移动护士应使用什么电话呢？可以使用思科无线 IP 电话或者是装有 IP 软电话的 PDA（手持智能终端设备）/智能手机终端等设备，这个 PDA/平板电脑可以根据呼叫者的主叫号码，系统自动从 HIS 等后台应用上调出呼叫病人的基本信息——姓名/体征信息如血型、最近的血压起伏变化、手术情况、近期服药情况、等，同时也是一个病人与护士的通讯工具。

2. 医疗导诊及信息发布系统

随着医疗体制改革的不断深入，医疗市场竞争愈发激烈。信息化、智能化大潮席卷了社会的每个角落，也唤起了人们对医院服务质量与信息化的更高要求。传统的医院导诊与信息发布管理模式已经跟不上卫生服务发展的需要，提高医院管理和服务水平，提升自身形象，提高全院的工作效率，提升医院的品牌效益和核心竞争力是做好公共事业的关键所在。

利用医疗信息发布系统能够优化就医流程，提高看病效率，让广大患者有序、轻松就医，解决医生工作受患者影响等问题，解决现有医院门诊医疗就诊信息提示不足、信息发布形式单一问题等。



该系统整合了传统的分诊排队及思科 DMS 流媒体发布与显示技术，能够与传统排队叫号系统无缝融合，实现了 LED、LCD 等多种信息发现形式、支持软硬件叫号。

- 智能引导功能

包括导诊排队叫号、分诊医生预约、门诊科室分诊、分诊导诊信息、取药引导、收费引导等。为各科室、挂号处、住院处等部门创造了轻松的排队环境，优化了排队秩序，提高了服务质量和管理水平；

- 进程即报功能

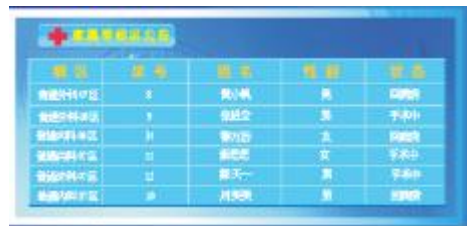
包括车位信息、各科室排队等候信息、手术进程信息的即时通报等。车位信息即时通报有利于间接疏导交通、人流；科室排队等候信息即时通报让病患随时了解各科室排队等候状况，以便自主安排时间选择就诊次序；手术进程信息的即时通报可让手术病患家属也用手术进程，舒缓家属紧张情绪；

- 结果反馈功能

包括检验、影像等领取报告的通知，让患者第一时间获得检验报告领取通知，不需要病人频繁到窗口咨询，同时也减轻了医护人员的工作强度。

门诊科室		
科室名称	排队等候人数	预计等候时间
内科	5 人	25 分钟
妇产科	2 人	40 分钟
消化内科	3 人	18 分钟
外科	6 人	10 分钟
一樓收费处	4 人	18 分钟
二楼收费处	3 人	15 分钟

今日出诊专家				
序号	姓名	所属科室	时间	备注
一	张明	内科	上午 8:00	1 人
二	李华	外科	上午 9:00	2 人
三	王强	妇产科	上午 10:00	3 人
四	赵伟	儿科	上午 11:00	4 人
五	孙丽	眼科	上午 12:00	5 人
六	陈刚	耳鼻喉科	上午 13:00	6 人
七	周敏	口腔科	上午 14:00	7 人
八	吴昊	皮肤科	上午 15:00	8 人
九	郑宇	放射科	上午 16:00	9 人
十	冯磊	检验科	上午 17:00	10 人



• 信息发布功能

系统能通过大屏幕液晶或等离子电视播放电视或视频、图片、字幕等信息。医院将服务指南、医疗价格、医疗技术、医疗器械等发布在屏幕上，让来院患者在院期间“轻轻松松就医、明明白白消费”的同时，还能够在等待中放松心情，欣赏到精美的视频、接受医疗常识培训，也加深对医院的了解。



3. 远程医疗、培训以及会议系统

随着人口持续增长以及环境的恶化，需要提供医疗服务的病患或亚健康人群数量越来越多。在某些地区，特别是一些医疗资源匮乏的医疗机构正面临越来越大的压力；在大部分较边远及医疗资源有限的医疗机构中，医疗专家显得如此珍贵稀少。很多患者不得不长途跋涉前往区域中心较高级别的医疗机构寻求帮助；

因此，医疗行业需要向一个新的愿景迈进，即让整个医疗行业的所有成员都能够无缝地连接交互的数据、信息、知识和流程，从而降低成本、提高医疗行业生产率和提供更好的医疗服务。多媒体协作医疗就代表了这样的愿景。多媒体协作医疗有助于在医疗行业成员之间建立起协作式的关系，提供安全的、价格低廉的、便于获取的医疗服务。思科一直致力于通过交互式的流程、技术和人员，建立起医疗社区的协同，从而实现随时随地提供重要医疗信息的目标。

近年来，远程医疗的概念逐渐被医疗行业用户所提及，所谓远程医疗是指通

过计算机技术、通信技术与多媒体技术，同医疗技术相结合，旨在提高诊断与医疗水平、降低医疗开支、满足广大人民群众保健需求的一项全新的医疗服务。目前，远程医疗技术已经从最初的电视监护、电话远程诊断发展到利用高速网络进行数字、图像、语音的综合传输，并且实现了实时的语音和高清晰图像的交流，为现代医学的应用提供了更广阔的发展空间。

远程医疗包括远程医疗会诊、远程医学教育、建立多媒体医疗保健咨询系统等。远程医疗会诊在医学专家和病人之间建立起全新的联系，使病人在原地、原医院即可接受远地专家的会诊并在其指导下进行治疗和护理，可以节约医生和病人大量时间和金钱。远程医疗运用计算机、通信、医疗技术与设备，通过数据、文字、语音和图像资料的远距离传送，实现专家与病人、专家与医务人员之间异地“面对面”的会诊。远程医疗不仅仅是医疗或临床问题，还包括通讯网络、数据库等各方面问题，并且需要把它们集成到网络系统中。

利用思科提供的无边界远程会议系统，我们可以为中小型医院的远程医疗勾勒出一个完整的应用场景。整个场景分为院内及院外两个部分，院内使用网真系统、移动高清视频系统、应急指挥系统等连接院领导、专家、医护人员；院外通过运营商的链路连接各个地市县的分支机构以及互联网上各个专家及病患。在特殊情况下，也可以使用卫星链路作为应急指挥时的特殊数据及视频通道。针对中小型医院，可以根据规模及成本，从整个系统中选择相关设备，按需构建满足自身需求的远程医疗系统。

无边界多媒体协同医疗会诊系统

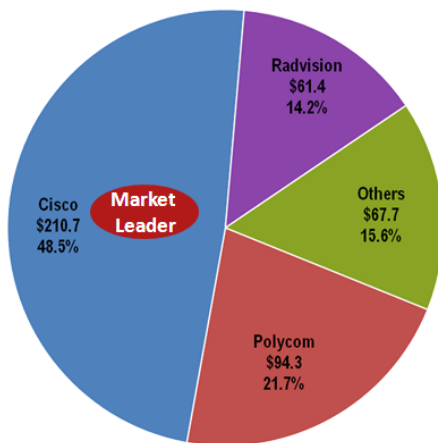


针对中小型医院的协同医疗应用，思科提供两类产品解决方案，包括 Cisco Tandberg 视频通讯解决方案及 Cisco Webex 协同会议系统解决方案。

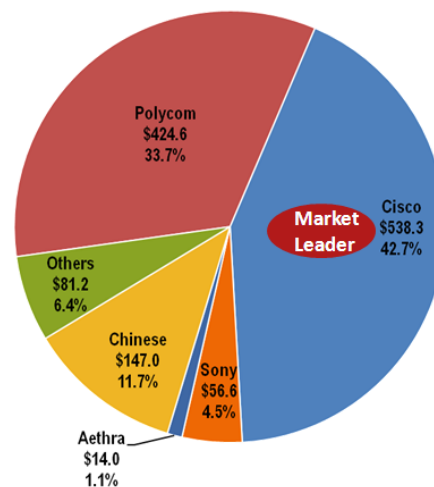
1) Cisco Tandberg 视频通讯解决方案

在 2009 年，Cisco 收购了原全球市场占有率第一的 Tandberg，将其视频通讯产品纳入到思科的协作通讯平台中，使得 Cisco 在 2009 年成为了全球视频终端和网络设备的领导者。

全球网络设备收入, \$Millions
100% = \$434M



全球视频终端收入, \$Millions
100% = \$1,262M

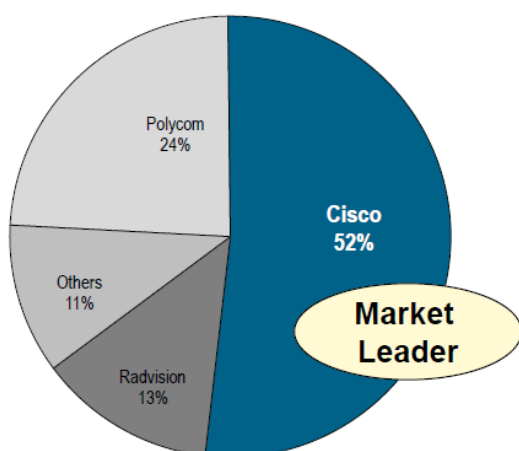


占全球市场的44% 市场份额!

根据 Wainhouse 最新给出的 2010 年第一寄到统计数据，Cisco 在视频终端产品市场占据了 45% 的份额，而在视频后台架构产品市场更是占据了 52% 的份额，超过市场份额的一半，远远超过其他竞争对手，对市场有主导能力。

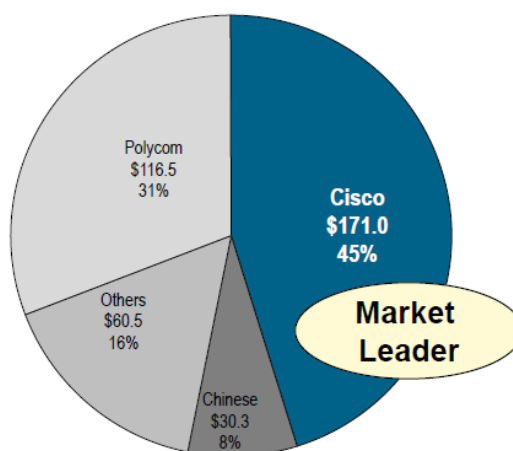
Q110 Global Infrastructure Market: Cisco Maintains #1 Market Share in all categories

Global Total Infrastructure Revenues, \$M
100% = \$120.4M



- Others include: Huawei, ZTE, Kedacom, Compunetix and other smaller vendors

Global Endpoints Revenues, \$Millions
100% = \$378.4M



- Others include: LifeSize, Sony, HP, Teliris and other smaller vendors
- Chinese Vendors are: Huawei, ZTE, H3C and Kedacom
- Chinese vendors are particularly strong in China, with some presence in CALA market as well, but little to no presence in N. America and EMEA

Source: Wainhouse Research Quarterly Spotcheck Reports, Q101 – Q110

Cisco 公司一直致力于视频通信技术和产品及系统的研究开发，并且是 ITU-T、IETF、IEEE 等视频通信标准的制定者之一，在视频通信领域拥有超过 1000 项的首创及专利技术，重要的技术标准有：

- 首先研发和应用 H.264 视频技术
- 首先研发和应用双流技术（后被 ITU-T 采纳成为 H.239 双流标准）
- 首先研发和应用防火墙穿越技术（后被 ITU-T 采纳成为 H.460 防火墙穿越标准）
- 首先应用数字高清 DVI 和 HDMI 接口技术；
- 首先应用 AAC-LD 高保真 CD 级音频技术；
- 发起和制定 MediaNet 技术，使视频与 IP 网络融合更紧密，网络自动识别和适应视频设备，自动进行 QoS，网络带宽配置优化；
- 发起和制定 TIP（网真系统互联协议）

Cisco 可以将视频通讯贯穿到整个协作解决方案中，可以为行业用户提供：IP 通讯、移动应用、客户服务、网真、协作会议、即时消息和企业门户软件的 7 种不同应用，并且 Cisco 的理念是能够将这些不同类型的应用进行融合，实现高度的统一协作通讯。

视频贯穿整个思科协作方案



利用 Cisco Tandberg 视频解决方案，能够给用户带来以下体验：

- 日常会议

日常会议是系统的主要应用模式之一，用户可以通过 MCU 会议预约功能，或者通过 TMS 的统一会议预约和管理平台，进行会议的安排、定制，用户无需根据组会模式的不同，而去选择不同的操作方式。相反，用户只需按时到达视频会议会议室就可和远端的同事进行探讨、交流。系统会根据这些信息，到时间自动开启与会的会场。

对于中小型医院用户，可充分利用这套系统召开所有分支机构高清视频会议，1080P 高清的画质加上 CD 级音箱的效果，足以让所有人感受如同在同一会场进行会议磋商。提高办公效率，为医疗会议保驾护航。

- 医疗应急指挥

出现突发事件，医院可以及时向政府主管部门进行最新疫情情况、最新技术发展及某项疑难课题研究的最新进展等，通过该高清系统可以和应急指挥中心进行无缝的对接，医院领导可第一时间对紧急情况会商、部署，以便政府部门对医疗卫生领域中安全性事件的应急性处理进行相关调度指挥。

- 领导会议

Cisco Tandberg 产品全高清的系统，不仅可以实时高清的传送本地全局会场画面，强大的 12 倍 1080P 光学变焦的摄像头还能捕捉到人的面部表情，甚至颜色。领导可以通过该系统随时随地的和其它部门同事进行沟通，从而增加决策的

效率。

- 医疗教学及手术观摩

实现专家将最新和最先进的医疗信息技术通过远程医疗系统传达给各个医院的医务人员，扩大了授课范围促进了医疗技术的交流，对各个医院的医务人员更新医学知识、提高个人素质、提高医疗水平起到了积极的促进作用。

同时可以实现医务人员足不出户就能清晰、真实的观摩到世界各地顶尖医学专家的现场手术过程，还可将手术过程录制下来，有利于学习和保留。避免了地域和手术室观摩人数控制指标的限制，有利于提高实习医生的学习质量。

此类型的培训/讲座可以两种类型：一种是会场型培训，一种是基于 PC 的桌面型培训。也可以是两种培训形式相结合。

会场型培训，可以通过 MCU 会议管理功能或者 TMS 预约的方式，把需要参加培训的会场呼叫进入培训会议室，然后参加培训人员进入会场，演讲者直接在自己所在的会场发送培训内容双流，并进行讲解。培训人员可以在看到课件的同时看到演讲者。

另一模式是桌面型培训，这种方式实际借助了 Cisco-Tandberg MCU 独有的软视频 ConferenceMe 功能，或录播服务器高清直播功能。只需要演讲者预定一个会议室，培训人员通过 WEB 界面加入会议，观看会议直播，直播内容包括了讲师的音视频，以及培训内容，如果与会人员有问题也可以与讲师互动或直接将电脑桌面双流发送给讲师。

这种模式适合于大规模培训，或者是当培训和日常大会发生冲突的时候，需要参加培训的用户可以直接在自己座位上，通过 PC 参加培训。

- 远程诊断及会诊

使病人在城里不用出社区，在农村不用出乡镇即可接受到有专科优势医院的专家进行诊断并在其指导下进行治疗和护理，最有效的利用资源，用最便捷的方式为患者提供诊断服务。

对于疑难杂症的病人，当地的主治医师可以通过系统向会诊中心提出申请，并与中心联系确认邀请的专家及时间，同时将病人的病例及各项辅助检查资料通过系统传给专家所在的远程医疗中心。诊治时，专家和患者可以通过系统进行“面对面”的交流，专业医学数据的会诊分析，再由当地主治医师与专家团进行互动交流，最终做出正确的诊断，使患者得到更为有效和合理的治疗。

利用此方式可以节约医生及患者的时间，并节省远程医患旅途费用。

- 移动会议

借助 Cisco Tandberg MCU 独有的 ConferenceMe 功能，无论用户是在办

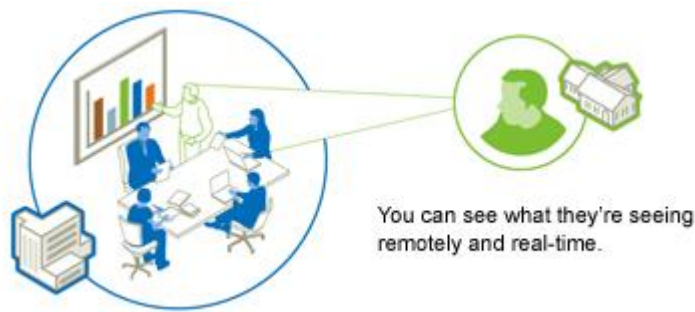
公室、家中还是在宾馆，只要接入到公司网络中，就可进行视频会议了，对于医院用户来说，在一些突发的事件中，这一功能将起到至关重要的作用。

2) Cisco Webex 协同会议系统

医院有非常多的培训和会议需求，如医院内部，医院与医院之间以及医院与大学的医学院之间都有非常多的会议和培训，传统的这些会议和培训往往需要大家集中到特定的地方在特定时间才能进行，而且浪费大量前往会议或者培训地点的时间。而且这些会议和培训也不容易保存下来。思科 Webex 系统很好的解决了医院的这一难题，只要你的电脑能上网，就能进行一个培训或者是召开一个会议，而且会议和培训内容是可以保存和回放的，医院要做的只是申请一个 webex 的帐号，就可以在网上建立一个虚拟会议或者培训室。

- 网络会议

Cisco WebEx 与世界各地的人们共享文档、进行演示和协作。网络会议让您能够借助因特网的力量举行会议而无需离开您的办公室。



WebEx 领先的按需网络会议。现在我们提供专用网络会议解决方案，专为整个客户销售周期的业务功能而优化。无需安装软件也无需购买硬件。无论您使用的是何种平台，您都只需单击鼠标即开始网络会议。与全城乃至全世界的人们合作，如同他们就在您身边一样轻松。只需打开您的 Web 浏览器启动 WebEx 网络会议就可以随时随地与任何人进行通信和协作。您的在线会议是私人的，且您的桌面隐私也在您的控制之下。

随时向任何人演示产品和服务。显示 PowerPoint 演示、高亮显示产品功能以及查看合同和文档。通过借助您的桌面网络摄像头启用视频功能来个性化您的销售会议。

实时查看、注释或编辑文档并进行自主的“问与答”会话。计算预算、就演示材料进行协作，同时节省了差旅费用及其带来的不便。就任何主题向遍布全球的员工提供实时、具时效性的交互式培训。就流程更改、规章制度以及公司范围内的创新事宜来培训员工，避免了出差所带来的各种不便。向客户或员工快速提供软件展示及解决支持问题而不受地理位置限制，就如同他们身在现场一样。管理分散在各地的项目团队，使用安全即时消息传递进行快速通信，然后在您需要

共享文档时即加入到网络会议中，以此来建立更紧密的联系。

- 视频会议

视频会议过去需要专门的会议室、培训设备操作技巧并且提前通知和预约才可以主持。借助 WebEx 则无需安装软件也无需购买硬件。您可以从桌面安排即时随需会议，您甚至还可以从我们的安全业务即时消息程序开始这些会议。现在，您可以通过一种易于使用的随需服务来获取主持网络会议所需的一切。



增添强大的演示功能。在您通信时提高和拓宽您的视角，就如同和客户、合作伙伴或同事面对面一样，无论和对方是否处在同一座大楼或身在何方。共享文档、视频甚至是在需要时共享您的整个桌面，所有这些活动都是在保护您隐私的情况下进行。WebEx 已获得 WebTrust、SAS70 和 FDA 21 CFR Part 11 认证，确保您受到最高级别的安全性保护。

无论您的参加者身在何处，都可以向其展示新产品、主持全体员工大会以及协商下一季度的预算。无论参加者是三人还是三千人，您都可以用同样简单易用的服务进行演示。网络会议是全体员工大会及小型团队协作的理想之选。开始于安全即时消息传递并可无缝升级至在线会议。

演示产品并使用附加的白板、聊天和投票功能以获得即时的反馈并确保您的消息传达。通过共享您的桌面及桌面上的任何内容，无需向服务器上传文件即可在任一应用程序中进行共享和合作，从而实现与他人协作。通过利用多媒体对象、Flash™、流式播放音频和视频以及 3D 图形，可以多样的风格呈现您需共享的内容。

网络会议提供实时会议品质的视频会议，无需高额成本、无需事先安排或占用专用会议室。您可以实现所有会议参加者之间更强的交互性和效用。WebEx 随需应用程序套件提供安全、丰富、集成的多媒体体验而无需预先资金投入。

- 音频会议

使用音频会议的 WebEx 帐户扩大您的电话会议功能。安排具有相同访问码的仅音频型会议和集成网络会议。使用相同的灵活呼叫选项和 Microsoft Outlook® 集成以简化安排程序。如果您离开了您的办公桌，则可以通过任一部

电话即时安排您的仅音频型会议。

借助集成的音频会议改进通信，同时加快商业决定：

- * 通过任何一部电话或从我们的安全即时消息传递客户端内为按需会议即时启动音频会议。
 - * 使用我们的“WebEx 与 Outlook 集成”及其它常用应用程序通过您的 WebEx 帐户安排在线电话会议。
 - * 通过对所有与会者进行视像验证并消除未授权的访问，保护您的对话隐私。
 - * 轻松管理音频访问如同您可以可见地控制所有电话会议活动、预先静音和激活音频线路以及轻松管理音频访问以创建超级的会议体验。
 - * 在当今高速发展的社会中，保持联系已变得日益重要。借助方便快捷且简单易用的音频会议解决方案为您和您的参加者动态增强网络会议体验。
- 网络研讨会和网络广播

使用网络研讨会和网络广播从您的活动和市场营销预算中获得更多收益。使用网络研讨会生成销售线索、举行公司全体员工大会以及为分散在各地的客户和学生培训。网络研讨会和网络广播让您能够通过网络会议在公司内外轻松进行通信。在您开始学习网络广播时，定义一些术语可能会有所帮助。



网络研讨会是一种具有交互性元素的在线研讨会或演示。您可以与观众进行互动，让人们“举手”提问、进行投票及更多操作。网络广播是一种不需要交互的演示，就像观看电影而不是参与讨论。

网络研讨会允许您“接触”世界各地的人们而无需承受出差所带来的不便及昂贵经费。以更少的时间与更多的人进行连接和协作。您还可以录制您的网络研讨会并在稍后播放，以便那些未能出席实时活动的人仍可以观看和学习。以下是指导您快速入门的一些技巧。

创建回答问题或解决问题的有用内容。请勿创建对您的服务或产品起不到任

何商业推广作用的网络研讨会。聘请知名专家为您的研讨会提供更多价值。著名发言人可以帮助您吸引与会者注意,特别是聘请您的组织之外的知名专家则效果更佳。

选择每周最合适的一天以及当天最佳时间,可以接触到最多的人。周二到周四一般会吸引最多的与会者,但不要将您的网络研讨会安排在重大节日或行业活动前后。如果您的目标观众横跨多个时区,则时间选择更为重要,可引导我们最终做出正确选择。

提供重复的演示。如果您可以提供多次出席您的网络研讨会的机会,则您很可能会吸引更多的人参加。如果您无法提供多个实时演示,则可以考虑录制活动并在稍后作为网络广播提供。

通过您的日常渠道(包括报刊杂志和广告)推广您的网络研讨会和网络广播。确保您至少在活动开始前 30 天就已着手这些推广活动。请勿在此推广阶段包含您现有的客户群。您的销售人员可通过电子邮件或电话向现有客户发送个人邀请,从而大大提高了生产力。确保您已制定了快速且轻松的注册流程。在活动开始前向所有已注册的参加者发送确认电子邮件并进行为期一周的跟踪提醒,此外,在活动开始前一小时再进行提醒才可确保活动获得最高出席率。

通过在与会者退出网络研讨会时向其提供调查问卷可获得有关您活动的即时反馈以及与会者的兴趣爱好。您还可能希望跟踪那些已注册但尚未出席的与会者。如果您再次提供此网络研讨会,则可确保让该群体都能够了解会议情况。如果您已录制了该网络研讨会且稍后将作为网络广播提供,则请确保包含有关网络广播的信息。

4. 病人监控系统

我们都知道,护士在某个时刻只能出现在一个地方,但是,繁忙的工作却时时把她们当成超人使唤。随着医疗机构规模的继续扩大,护士们将需要在更短的时间内护理更多的病人,而且护理质量不能有丝毫下降。与此同时,护士还必须时刻保持自身的心智健全。幸运的是,她们现在可以使用病人监控系统。

利用病人监控系统,移动员工能够随时查看病人数据,并监控医院内的所有设备。只需按一下按钮,护士就可以在医院的任何地方用文字和图形格式快速查看任何病人的监护设备,浏览任何病人的发病史,并拨打电话询问检查结果,甚至能够制定病人警报标准。不仅如此,由于每次访问时,系统都能够对电子病历进行更新,因此,即使在护士换班时,病人也能得到一致的护理。所有资料都清晰、简洁,有利于护士提供快速、有效、统一的护理。

利用病人监控系统,护士不需要进入病房就可以预先了解每位病人的病情,因而可以根据病情的严重程度作出适当的反应。现在,护士不必再作飞来飞去的超人,只需要出现在最需要的地方即可。

二、 思科协作解决方案设备参考

- **Unified Communication Manager** （语音呼叫处理器）
 - MCS7835 每台支持 2500 门电话
 - MCS7825 每台支持 1000 门电话
 - MCS7816, 每台支持 500 门电话
 - UCS C 系列服务器
- **Unified Communication Manager Express**
 - Cisco ISR G1/G2 系列 CCME
- **终端 IP 电话**
 - CP-7985-PAL 视频 IP 电话
 - CP-7975G 彩色触摸屏 IP 电话
 - CP-7942G 黑白大屏幕 IP 电话
 - CP-7911G
 - CP-6900 系列 IP 电话
 - SW-IPCOMM-E1 软件电话, 安装于 PC
- **语音网关**
 - Cisco ISR G1/G2 系列
 - VWIC2-2MFT-T1/E1 E1 语音中继卡, 连接 PSTN 或者 PBX
 - VIC-4FXS/DID 模拟语音接口卡, 连接传统模拟电话
- **DMS 数字媒体系统**
 - 数字媒体编码器
 - 数字媒体管理系统
 - 数字媒体播放器
- **Tandberg 视频会议系统**
 - Cisco Tandberg C20/40/60/90 高清终端
 - Cisco Tandberg EX60/90 个人桌面高清网真终端

- Cisco Tandberg E20 Voip 视频电话
- Cisco Tandberg 4500 MCU
- **Webex 会议系统**

详细信息欢迎垂询思科区域中小企业客户经理和中小企业客户技术支持工程师，或参考思科网站：

- **English: www.cisco.com**
- **中文: www.cisco.com.cn**

第七章 思科统一计算在医疗行业的应用

当前，医疗行业数据中心存在着各应用系统无法有效融合、设备重复投资、设备性能利用率不高、系统稳定性不一等问题。造成这些问题的其中一个主要原因是各种应用程序未能与执行它们的物理运算平台有效分离。而虚拟化技术正是解决这一问题的有效途径，通过把应用程序部署在一个多个统一的物理服务器资源池中，虚拟化能够带来以下的优势：

- 整合工作负载；提高利用率；降低运营、投资、空间、耗电和冷却等。
- 在虚拟池中动态地移动工作负载，提高使服务器离线或增加新服务器的灵活性。
- 管理虚拟机与物理机之间的关系，优化性能，保证服务水平。
- 使用现有资源池创建更多虚拟机，从而扩展当前应用或部署新应用。
- 使用虚拟化软件的高可用性和灾难恢复功能，来解决本地和跨地区故障问题。

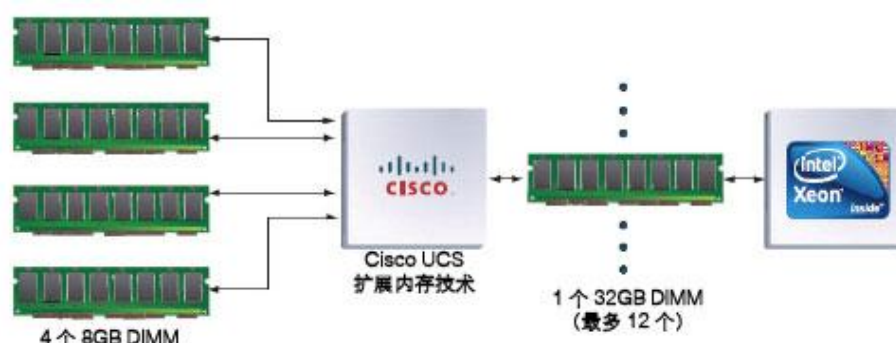
思科统一计算系统就旨在提供这样一个环境。专为虚拟化环境而优化的思科统一计算系统是下一代数据中心平台，在一个紧密结合的系统中整合了计算、网络、存储接入与虚拟化功能，旨在降低总体拥有成本（TCO），同时提高业务灵活性。该系统包含一个低延时无丢包万兆以太网统一阵列，以及多台企业级 x86 架构服务器。它是一个集成的可扩展多机箱平台，在统一的管理域中管理所有资源。

虚拟环境需要一致的 I/O 配置，为资源池中所有服务器的系统管理程序提供统一支持。它们还需要能够支持虚拟机（VM）在资源池中的各服务器间移动，同时又能满足各虚拟机带宽和安全要求的 I/O 配置。思科统一计算系统以一个低延时无丢包的 10-Gbps 统一网络阵列为基础，能够满足这一需要。此统一阵列不再需要在每个服务器中部署冗余以太网和光纤通道适配器，也不必采用独立布线连接接入层交换机，并为每种网络媒体使用不同交换机，因此大大简化了机架布线。所有流量都路由到中央服务器互联，随后以太网和光纤通道流量可独立传输到本地非整合网络。

当服务器配置到资源池中以后，便可以根据需要进行管理，以满足不断变化的工作负载要求；在部署新应用时无需为其安装特定硬件；并能在服务器间移动虚拟机，以均衡工作负载、满足服务水平协议(SLA)或使某个服务器为计划内停机作好准备时，虚拟化能为数据中心发挥最大价值。Cisco UCS Manager 将思科统一计算系统的资源整合为单一综合系统，非常适于为虚拟环境建立资源池。

Cisco UCS Manager 是思科统一计算系统的中枢神经系统。它从端到端集成系统组件，因此系统能作为单一逻辑实体进行管理。Cisco UCS Manager 提供一个直观 GUI、一个命令行界面(CLI)和一个强大的 API，因此它能单独使用，也能与其他第三方工具集成使用。通过单一控制台，能够全方位管理服务器配置 – 系统身份、固件版本、网卡(NIC)设置、HBA 设置和网络配置文件等，无需每个系统组件配备单独的管理器。

虚拟化将更多关注服务器如何拥有更多以及更经济的内存配置，思科独创的扩展内存技术提供了最佳的解决方案。采用了思科扩展内存技术的 UCS C250 M1 机架式服务器将四个物理上独立的 DIMM 映射为单一逻辑 DIMM，在使用 8-GB DIMM 时最大内存高达 384 GB，从而能以更低 TCO 提高虚拟化密度，使医院的 IT 机构能够凭借更少资源完成更多任务。



(图) 思科扩展内存技术使 4 个物理 DIMM 对于 CPU 来说显示为单一大型逻辑 DIMM

思科统一计算系统将计算、网络、存储访问和虚拟化统一到一个综合平台中，进行集中管理，并使用 VMware ESX 服务器等虚拟化软件进行协调。该系统在一个万兆以太网统一阵列中集成了企业级服务器，提供了虚拟机和虚拟化软件所需的 I/O 带宽和功能。思科扩展内存技术为高度虚拟化所需要的大内存提供了一种极为经济的配置方法。最后，思科统一计算系统将网络访问层集成为一个能轻松管理的实体，在此实体中，能像物理链路一样配置、管理和移动虚拟机链路。

Cisco UCS C 系列机架安装服务器将思科统一计算系统创新技术扩展到了机架安装机型，包括一个基于标准的统一网络阵列、Cisco VN-Link 虚拟化支持和思科扩展内存技术。这些服务器既能在独立环境中运行，也能作为思科统一计算系统的一部分运行，使中小型医疗机构能够逐步部署系统，也就是按照最适合的预算方式和时间安排来决定所用服务器的数量。



按照中小型医疗机构的应用特点，数据中心服务器的部署和使用可以分为两个阶段：

首先，在现阶段应用相对简单、投资预算有限的条件下，独立部署 Cisco UCS C 系列服务器，在异构环境中提供业界标准的管理和应用特性。

当作为独立服务器部署在异构环境中时，Cisco UCS C 系列服务器能像其他任何 x86 架构服务器一样进行管理。无需修改，即能运行使用 OS 主机代理的常用企业管理工具。Cisco UCS 集成管理控制器为管理员提供了所需工具，帮助他们以手动操作的方式控制服务器功能，包括远程键盘、视频和鼠标 (KVM)，电源开关，以及用于系统监控的标准 SNMP 陷阱。

第二，在未来，随着医院信息化的进一步发展，C 系列服务器可以作为思科统一计算系统的一部分，提供了出色的投资保护。

C 系列服务器能够与思科统一计算系统集成，成为单一综合系统的一部分，由一个集成、内嵌、高度可用的安全管理系统管理。该系统采用与机型无关的架构，在资源使用方面提供了出色灵活性。Cisco UCS C 系列服务器能够根据需要在思科统一计算系统中调整配置，且能在该系统与 Cisco UCS B 系列刀片服务器一起运行。

使用这种分阶段的模式，中小型医疗机构能够按照自身的发展时机和预算情况，逐步部署系统，根据需要选择服务器数量。C 系列这种灵活的设计使其能够适用于广泛的数据中心环境，包括使用思科统一计算系统、Cisco Nexus 系列产品、以及来自思科和第三方的独立以太网与光纤通道交换机的环境。



图：C 系列服务器在各种数据中心环境下的灵活部署

与传统的机架式服务器相比，思科 C 系列在广泛的应用环境下提供了多种独特的优势，包括：

- Cisco 扩展内存技术

相比传统的双路 CPU 服务器，这一技术可带来两倍的内存空间（384GB），并能够通过使用 4 GB 而非 8 GB DIMM 实现更为经济的（192 GB）内存空间。它用于针对虚拟化和大数据集工作负载的需求，在处理能力与内存容量之间实现最佳平衡，让企业无需再为了提供更大内存空间而升级到昂贵的四路 CPU 服务器。同时，它还能够帮助降低资本开支与运营成本。

- 灵活的 I/O 与存储选项

该服务器拥有 5 个 PCI Express (PCIe) 扩展插槽，提供了出色的 I/O 灵活性和带宽，能够全面集成传统千兆以太网 LAN 和光纤通道 SAN。服务器配备了多达 8 个内部小型 (SFF) SAS 或 SATA 驱动器，其内部存储容量远远高于同类刀片外形服务器所能提供的水平。

- 万兆统一网络阵列

当配备了融合网络接口 (CNA) 或 Cisco UCS P81E 虚拟接口卡时，该服务器可以集成低延时无丢包 10 Gbps 以太网与工业标准以太网光纤通道 (FCoE) 阵列。这一技术支持“一次布线部署模式”，这意味着变更 I/O 配置不再需要安装相应的板卡，并对机架及交换机重新布线。

- 虚拟化优化

思科 VN-Link 技术、I/O 虚拟化和 Intel® Xeon® 5500 系列处理器将网络直接延伸到虚拟机。这一优化能够支持实现一致、可扩展的操作模式，帮助提高安全性和效率，同时降低复杂性。

- 统一管理

当集成至思科统一计算系统作为其一部分使用时，管理功能将被集成到系统的所有组件之中，通过 Cisco UCS Manager，管理整个解决方案就像管理一个单一实体一样，从而显著提高运营效率与灵活性。

- 服务配置文件

当集成作为思科统一计算系统的一部分时，Cisco UCS Manager 可使用服务配置文件和模板实施基于角色与策略的管理。服务配置文件可帮助自动化配置和增加业务灵活性，让数据中心经理能够在短短几分钟内完成应用配置，无需再花费几天的时间。

常用的思科统一计算 C 系列机架式服务器如下：

产品系列	说明
Cisco UCS C200 M2	2 路服务器，部署通用计算
Cisco UCS C210 M2	2 路服务器，部署通用计算
Cisco UCS C250 M2	2 路服务器，内存增强型应用，部署高密度虚拟机
Cisco UCS C460 M1	4 路服务器，CPU/内存增强型，部署关键业务/高可靠应用

详细信息欢迎垂询思科区域中小企业客户经理和中小企业客户技术支持工程师，或参考思科网站：

- **English:** www.cisco.com
- **中文:** www.cisco.com.cn

第八章 结束语：医疗行业用户为什么选择思科

医院如何更好地服务社会是各级各类医院关心和关注的首要问题，“一流的医院，一流的服务，需要一流的软硬件环境”，网络作为医院核心业务应用的基础承载系统，其可靠性和安全性变得尤为重要。作为领先的网络厂商我们一直非常重视和配合医院业务和体制变革所带来的挑战和变化，国内很多医院在过去的几年的时间里纷纷把网络系统换成高品质的思科网络设备和解决方案，这已经成为医疗行业用户网络设备选型主流的发展趋势。技术先进、成功案例、全面的解决方案、厂商的生命力、投资保护和售后服务支持能力是医院网络设备选型需要考虑的主要因素，除了医院重要的核心医疗业务应用需要运行在高品质的健壮的网络平台上这个原因之外，思科还以以下优势为医疗行业的用户提供更好的服务：

- **思科医疗级高质量、高稳定、技术先进的网络设备和解决方案，保障医疗业务高可靠地运行，得到了业界的广泛认可。**思科产品以其先进的软、硬件设计，针对用户需求的研发方向，大量的研发投入和先进的生产质量控制等成为最高质量和最稳定的网络设备和解决方案，这也通过大量的医疗行业、金融行业和证券行业等用户的使用实践所证明，在这些对网络可靠性要求极高的行业中思科都具有大量的成功案例和极高的市场占有率。

- **思科具有大量的医疗行业用户成功案例和丰富的医疗网络建设经验。**鉴于思科产品的在行业内的领先地位和技术先进性，思科在医疗行业拥有大量的成功案例。思科拥有在国内外大量的医疗行业客户网络建设的实践基础，了解医院的应用和发展趋势，了解医院信息系统需要解决的问题，并拥有完整、独特、领先、有针对性的技术解决方案，因而具有丰富的医疗网络建设经验，思科通过解决方案的形式将这些经验分享给医疗行业的用户，为医疗网络建设提供咨询服务。

- **思科拥有全面的解决方案，满足医院现在和未来信息化建设发展的需求。**思科是业界领先的提供承载生命的信息系统——医院信息系统整体网络解决方案的厂商，我们不但能够提供适合医院业务系统的高可靠、安全智能的基础网络系统，还能提供满足医院全面信息化建设需要的统一通信、统一无线、自适应网络安全和新型医院数据中心等全面的解决方案，思科在以上解决方案方面拥有丰富成熟的国内外建设和应用的成功案例经验可以供国内医疗行业用户参考。

- **思科是业界专注于网络且具有很强生命力的厂商，可以为医疗行业用户提供持续不断的技术支持、技术升级和售后服务。**思科是全球网络和通信领域公认领先的互联网解决方案供应商，思科在全球的网络市场占有率及国内医疗行业的市场占有率都是遥遥领先的，财富五百强中 89% 是思科的用户，全球电信用户 95% 是思科的用户。思科通过不断的技术创新，一直以来都是网络行业具有很强生命力的引领网络发展方向的主流厂商。思科公司运营稳定持续增长，过去的一年思科的收入为 395 亿美金，研发投入 52 亿美金，思科公司的稳定发展和

大量的研发投入，可以保障为医疗行业用户提供持续不断的技术支持、技术升级和售后服务。

- **思科非常重视医疗行业用户的投资保护，使医疗行业用户具有较低的网络总体拥有成本。**如何更好的实现客户的投资保护一向是指导和修正思科产品研发和创新的指导思想之一，因此采用思科的整体方案具有较低的长期拥有成本（包括初次购买、运营维护管理、网络扩展、技术升级费用的总和），并能够通过减少宕机时间，使网络正常工作时间最大化，有力地支撑医院业务在网络上不间断地运行，避免给医院带来声誉和财务上的损失，并且提高医疗服务质量。思科产品具有顽强的生命周期，比如：思科 1999 年开发推出的 Catalyst 6500 平台，其中的模块和接口板现今仍然能够在最新一代的 Catalyst 6500 平台上使用。目前国内有很多三甲医院采用了思科的双 Catalyst 6500 交换机作为网络的核心交换机，为保证这些医院的全院网络可靠工作发挥了重要作用。

- **思科公司高效的服务体系，是医疗行业用户网络安全可靠运行的重要保障。**思科公司秉承“服务至上”的原则，开发了独具特色的全球支持模式，通过互联网为用户打开了取之不尽、用之不竭的支持资源库，帮助用户妥善解决在整个网络生命周期内遇到的各种网络问题。为了响应中国市场不断提升的网络服务需求，对中国本地客户提供更加全面和直接的支持，2006 年 5 月，思科系统公司在北京注册成立了思科系统（中国）信息技术服务有限公司，专注于为中国客户提供全面的网络生命周期服务，帮助用户对网络进行规划、设计、实施、运营和优化，以成功部署和使用网络技术，为思科向包括医疗行业在内的中国客户提供高效优质的服务提供了强有力的支持。思科还将继续在资金投入、技术引进、原料采购和生产等各个方面加大对中国市场的投入。

客户满意是验证思科服务的最佳标准，思科愿意在大量的国内外医疗行业网络建设实践的基础上，向医疗行业的用户学习，并愿意分享在此过程中不断积累的丰富的医疗信息化建设经验，思科将一如既往地与中国医疗用户共同迎接网络经济的美好机遇，进一步推动中国医院信息化建设进程。