



2

高可靠的医疗级基础网络设施 解决方案

2.1 医院对高可靠的网络的需求	07
2.2 系统高可靠性的定义	07
2.3 思科医疗级网络高可靠性解决方案	08
2.4 思科高可靠医疗级网络基础设施解决方案设备参考	13
2.5 思科高可靠医疗级网络基础设施解决方案客户成功案例举例	13

二、高可靠的医疗级基础网络设施解决方案

医疗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）、医学影像系统（PACS）、电子病历（EMR）、医疗一卡通和护士呼叫等。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极高的要求。

2.1 医院对高可靠的网络的需求

我们需要准备一个怎样的网络，才能满足医院对网络的需求？让我们先从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。

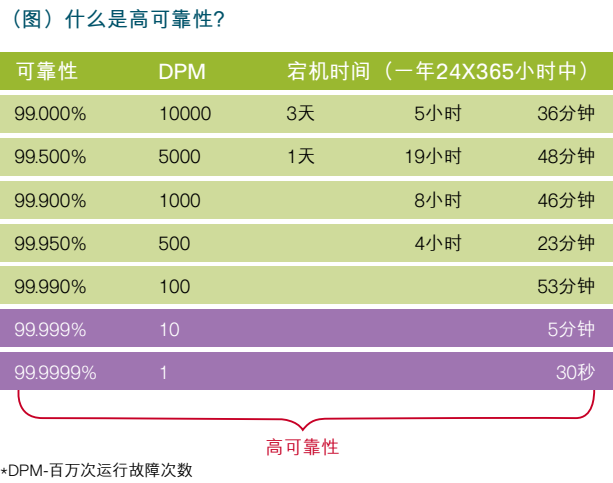
其他信息系统涉及对外连接，用户对远程资源的访问控制以及广域网链路服务质量是关键，因而对系统可靠性和安全性要求较高，需要同时支持语音、视频和数据等多种业务。

高可靠性是医疗网络的首要关注点。早在几年前，医疗网上就开始运行着重要的HIS等数据信息，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，但是不是必须采用双机备份的解决方案。

2.2 系统高可靠性的定义

可靠性的严格定义为系统在规定条件下和规定时间内、完成规定功能的概率。通常，对可靠性描述为其反面，描述为固定时间段内，系统无法正常工作的次数和持续时间，如下表。高可靠性通常指代系统能够实现99.999%以及以上的可用性，如下图所示：



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。

2.3 思科医疗级网络高可靠性解决方案

目前一部分医院网络现状主要呈现以下特点：

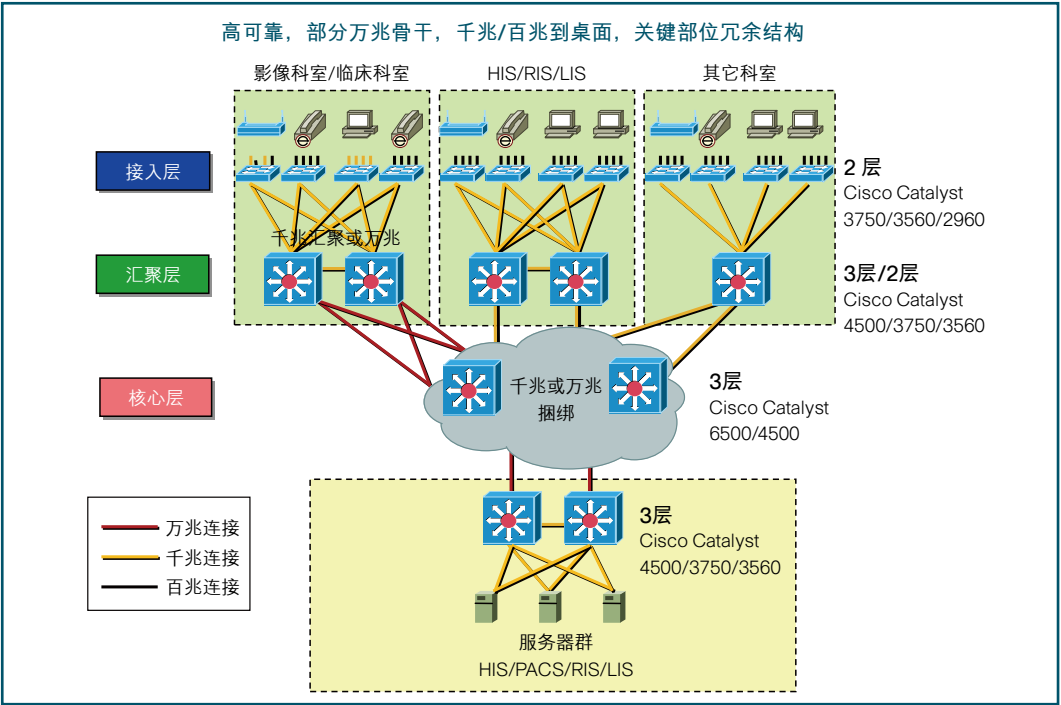
- 模块化，多层架构
 - 核心层、汇聚层和接入层架构 与 核心和接入层架构相结合
 - 双核心交换机（热备或冷备）
 - 单汇聚交换机（增加单点故障）和双汇聚交换机相结合
- 核心层具有路由功能，部分汇聚层具有路由功能
- 汇聚层或核心层负载均衡
- 少量VLAN跨越（部分网络没有划分VLAN）
- 千兆和百兆相结合

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。

1. 保障医疗级网络高可靠运行的架构

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。

（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ToPoint 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。负载平衡、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平衡协议（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。

2. 思科保障医疗级网络高可靠运行的网络技术

除了以上提到在结构设计层面实现可靠性外，在网络技术层面，包括设备级可靠，链路级可靠，以及网络级可靠。思科有非常突出的技术特点可以在这几方面实现高可靠性需求。如下图所示：

(图) 思科保障医疗网络高可靠运行的网络技术举例



设备级可靠性包括：

- 冗余、负载均衡电源（AC和DC）
- 冗余共享风扇
- 冗余系统时钟
- 冗余上行链路
- 冗余交换矩阵

- 包括电源、风扇、线路板模块、交换背板在内的所有系统单元都可热插拔，如元件增加、转移或替换，而不会导致相关业务中断。所有系统单元都可现场替换，从而实现了最大服务性和最少的网络停机时间。

网络链路级和网络层可靠性:

网络应能承受元件、链路、电源以及其它类型的故障。网络必须围绕这些故障收敛，自愈，而不干扰网络运行并使网络业务的中断最小化。一方面，网络应该能够完成所有这些任务，另一方面，它还要十分简单，以使一般网络管理人员都能配置、监视并管理网络环境。提供网络冗余的设备在网络正常运行状态下还要对网络有其他好处，比如负载均衡等。因此在网络设计中采用VSS虚拟交换技术在提供快速故障恢复的同时还可以极大的降低冗余网络的管理复杂度。

不同虚拟网或不同子网间的访问需要路由设备，局域网内的工作站或服务器都必须配置自己的默认网关。当默认网关出现故障时，不同虚拟网或不同子网间的访问不能进行。因此为了提高网络系统的可靠性，访问层和分布层的第三层交换机采用热备份路由协议（VRRPHSRP），在出现灾难性故障时，快速切换到备份系统。同时通过对备份优先级的控制，以及先进的网关负载均衡协议（GLBP）可以实现多台第三层交换机的负载均衡，即在正常运转情况下，每台第三层交换机同时各自为同一VLAN中不同的主机提供网关负载均衡服务。

以下将简单介绍部分思科高可靠网络技术：包括VSS技术，以及EEM技术，IP SLA技术，ERSPAN技术等。

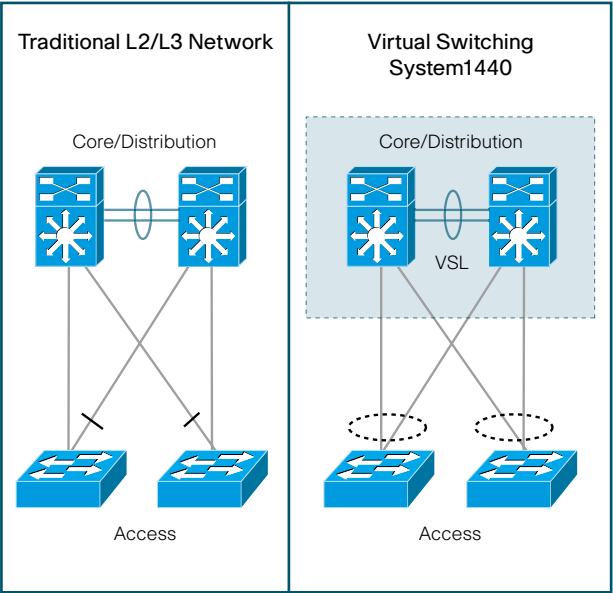
VSS技术:

VSS 即virtual switching system，虚拟交换系统，可以将多个Cisco Catalyst 6500系列交换机整合为单一虚拟交换机，通过跨机箱链路技术，增强了核心系统的可靠性。

使用VSS技术的原因在于通常对双核心设备的管理存在如下问题:

- 无法实现对双核心交换机的统一管理；之间需要进行复杂的配置；
- 接入或汇聚交换机通过双链路上连到双核心时，由于双核心交换机为单独两台设备，需要在三台设备之间运行生成树协议，上行链路中会有一条处于断开状态；
- 当上行链路出现故障时，需要进行生成树收敛，才能恢复汇聚或接入设备到核心的链路连接；

通过VSS技术，凭借增强的阵列功能，能在故障发生时，一秒内完成故障切换，从而快速切换到备用管理引擎。



使用Cisco VSS 1440实现系统虚拟化：核心层上游和下游邻居将把VSS看作单一L2交换节点或单一L3路由节点，从而减少L2/L3控制协议流量。分布层单管理管理员将使用单管理点配置和管理VSS，这其中包括用于两台物理交换机的单一整合配置文件。接入层多机箱提供链路捆绑，这两台物理Cisco Catalyst 6500机箱在其中一台交换机发生问题时，即使链路捆绑实际上是在两台机箱上终接的，也能看作仅在另一台交换机上终接。VSS 1440的系统虚拟化技术将多个Cisco Catalyst 6500系列交换机整合为单一虚拟交换机，将系统带宽容量扩展到1.4 Tbps。

VSS成员通过虚拟交换链路（VSL）连接。VSL在虚拟交换机成员之间使用标准万兆以太网连接（多达8条，以提供冗余性）。通过在720-10G或WS-X6708-10G模块的任意端口上使用万兆以太网上行链路，即能形成VSL。除在VSS成员间进行控制通信外，VSL也能传输普通用户流量。

使用VSS技术在可靠性和可管理性方面优势如下:

- 对两台核心交换机实现单管理点，包括配置文件和单一网关IP地址（无需HSRP/ VRRP/GLBP），即逻辑上可以认为是一台设备。
- 多机箱以太捆绑（MEC）创建了简单的无环路拓扑结构，汇聚层到核心的连接以及核心之间的连接不再依靠生成树协议（STP），而是直接按照以太捆绑通道来实现；链路的收敛不再需要经过漫长的生成树收敛过程，而是使用（802.3ad或PAgP）能在一秒内完成L2链路恢复。
- 将系统带宽容量扩展到1.4 Tbps：通过使用冗余Cisco Catalyst 6500系列交换机上所有可用的L2带宽，提供自动、精确的负载均衡。Cisco VSS 1440消除了因园区中不对称路由造成的单播洪泛现象，并能最大限度地发挥虚拟交换机中的所有万兆以太网端口的作用。

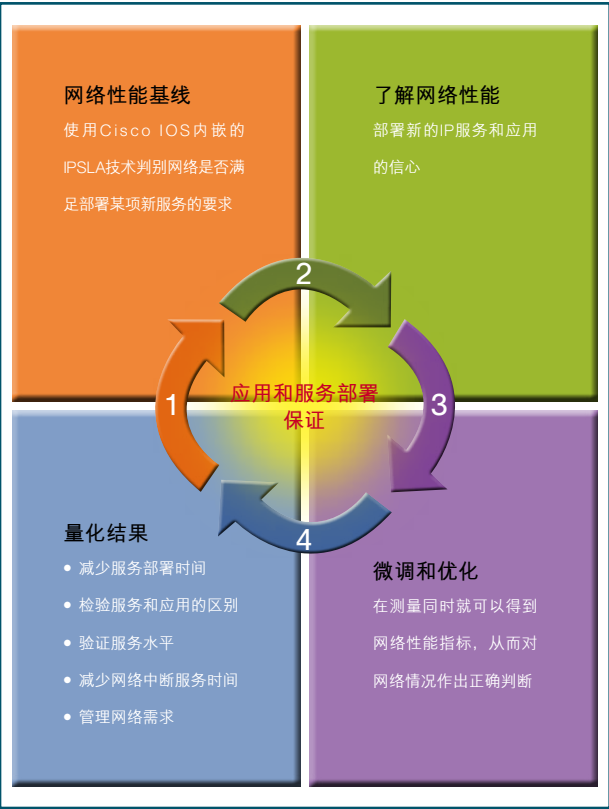
IP SLA技术:

IP SLA服务等级协议技术是思科领先的技术，并集成内嵌在大多数采用思科IOS的设备，包括思科3560交换机。通过IP SLA，能够实时收集网络性能信息：响应时间、单向延迟、抖动、丢包、语音质量数据及其它网络统计数据。用户能够以持续、可靠、可预测的方式测量网络性能，并主动监控网络状态。利用IP SLA，企业不但能自动执行服务水平监控，使IP服务水平得到保证，还能主动检查网络运营情况，并准确测量网络性能。主动监控能够持续测量网络中多条路径之间的网络性能，并提供持续性能基线。

用户在实际使用网络的过程中不论出任何问题，都是反映网络不行。在终端用户理解上，无论是网络连通性问题、还是服务器问题、还是应用软件问题他们都认为是网络平台出问题，他们天然认为网络就是代表一切。通过使用

IP SLA，就能实时地监控每一个终端用户到所有访问线路及服务器设备上的延时、抖动、丢包、拥挤的状况，也能实时模拟终端用户访问相应服务器，确定服务器的回应时间，从而分析出当用户反映网络有问题时，究竟是网络设备问题、还是某段线路问题、还是服务器的问题，并能整理出完整的报告。

（图）思科IOS IP SLA生命周期



EEM内嵌事件管理技术:

内嵌事件管理器（EEM）是集成在思科IOS路由器和交换机（包括3560交换机）中的一个非常有用的功能。EEM是一种事件检测和恢复工具，可为用户提供客户化的安全、可靠性等方面的增强能力。通过内嵌的大量事件检测工具，例如内存过高，线路误码太大，时间到等事件触发后，EEM将自动执行事先定义好的行为，例如执行一段代码，或发送通知，切换引擎等来自动修复网络故障，由此实现对高可靠性的保障。

通过EEM，可以为网络设备赋予更多的智能，提高管理效率，降低管理成本。EEM适用范围非常广泛，例如：

- 当内存占有率到95%，将流量交换到另一台交换机。
- 当链路错误高但是没有中断时，关闭该链路，使用冗余链路。
- 需要在晚上12:00使用更高级别ACL，第二天上班又使用普通ACL等等。

ERSPAN技术：

在日常网络管理中，有时需要使用IDS或流量监控设备来分析处理流量，这是就需要使用交换机上的一个功能：端口镜像（SPAN）来捕获网络流量。有时需要监控远端流量，将IDS设备或流量监控设备带到远端不太现实，这时就需要采用远程端口镜像功能，对于中间全部是二层的局域网环境，使用的是RSPAN功能。如果中间是三层的路由环境，则要使用ERSPAN技术，需要利用到思科6500交换机上的GRE功能才能实现。通过SPAN、RSPAN和ERSPAN功能的有机结合，网管人员在网络中心就可以方便的监控网络中任意点的网络流量，从而有效管理网络，保障整体可靠性。

3. 建立医疗数据中心的存储整合和数据灾备

（详见本文第五部分：医疗级数据中心解决方案）

2.4 思科高可靠医疗级网络基础设施解决方案设备参考

- 核心层（两台）
 - 6500系列交换机
 - 4500系列交换机
- 汇聚层（两台或者一台）
 - 4500系列交换机
 - 3750系列交换机
 - 3560系列交换机
- 接入层（若干台）
 - 3750系列交换机
 - 3560系列交换机

- 2960系列交换机
- 数据中心交换机（两台或者多台）：
 - Catalyst 4900交换机
 - Catalyst 3750交换机
 - Catalyst 3560交换机

详细信息欢迎垂询思科区域医疗行业客户经理和医疗行业客户技术支持系统工程师，或参考思科网站：

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

2.5 思科高可靠医疗级网络基础设施解决方案客户成功案例举例

北京大学第三医院

1998年北京大学第三医院首次部署全院园区网络就采用了思科系统公司的网络设备，2001年再次扩容时仍然选择思科。最近，北医三院又对网络进行扩容升级改造，北医三院第三次牵手思科。“我们与思科有良好的互动和相互了解，”沈韬主任介绍，“更主要的是思科的综合实力、品牌和产品支持让我们现有的投资能够得到可靠保障。”

思科的网络解决方案以千兆以太网为主干、百兆到桌面，保证了医院高速度、高可靠性的数据传输要求。在安全方面，思科多层次深度防护的自防御安全系统解决方案，既能对医疗网络提供全面的安全防护，又不会因性能损失造成瓶颈。对北医三院以后的应用规模，网络解决方案具有充分的后续扩容能力。只需通过简单地添加模块或软件升级，即可实现平滑升级到高密度万兆性能，升级到高性能防火墙等功能。“我们现有的网络平台可以满足未来至少3到5年内业务扩展的需求。” 沈韬主任说。

华西医院

早在2004年，华西医院就已经完成了医院园区网络的阶段性建设，形成了以百兆为主、千兆为辅的光纤主干网。整

个网络接入了近千台客户端，支持以数据传输为主的医院信息系统、办公系统的运行，也为工作人员、学生和部分家属区提供互联网接入。

在之前的网络建设过程中，华西医院一直采用思科的路由器、交换机和防火墙等多种网络设备。华西医院信息化负责人黄主任表示：“思科在整个过程中给了华西医院大力的支持，包括针对医院的需求组织工程师上门系统讲解，帮助医院的工程技术人员更好的认识、了解、选择、配置思科的产品并应用于管理。”良好的合作关系促成了进一步的协作，思科被华西医院选定为其规划并部署更高性能的医院骨干网络架构。

基于思科提供的骨干网，华西医院将部署PACS系统等高信息吞吐量的解决方案。华西医院信息化负责人黄主任表示：“面对危急病人，我们将可以保证在他被送进手术室之前，他的检验片子就已被送到医生的电脑上，这使我们可以对他展开‘争分夺秒’的抢救工作。”。思科根据其需求特点，核心网络采用配以万兆端口的两台Cisco 6509交换机，各大楼主要汇聚层交换机采用Cisco 4507R，配以双万兆引擎和双电源冗余。为了保证网络安全性，中心机房两台核心交换机上配置了IDS模块，以实现实时入侵检测。同时，该网络通过使用思科安全监控和响应系统(CS-MARS)实现安全信息收集和攻击路径实时分析。在网络出口，还应用了SCE流量分析监控设备。

上海第二医科大学附属瑞金医院

上海瑞金医院原是国内著名的三级甲等综合性教学医院，在医疗、教学、科研、管理等方面在全国卫生系统名列前茅。作为全国医疗卫生行业的领先医院，瑞金医院自1985年以来，就不断投入计算机辅助管理系统的建设，较早实施了HIS、PACS等核心医疗应用，对整体网络提出了更高的要求。

瑞金医院采用3台Cisco 7600和1台Catalyst 6500，分别分布在2栋不同的楼宇中，形成全院的网络核心，并实现异楼双核心冗余备份。此外还采用了多台Catalyst 4500、Catalyst 3750、Catalyst 3500作为汇聚层交换机。全院汇聚和骨干之间通过路由连接，提高了网络的可靠性。

在PACS网络中全部采用千兆接入交换机。存储设备采用光纤通道存储局域网络（SAN）和光纤网络存储（NAS），以保证医院对大容量、高速度、高可靠扩充性的数据存储要求。

另外，瑞金医院还在病房、急诊楼中部署了思科无线产品，为病人、医生提供更便捷的医疗服务。