# 医院信息化网络设计与实现

蔡东江 吴平凤

（中山大学附属第五医院设备科 珠海 519000） （北京大学深圳医院设备科 深圳 518035）

〔摘要〕 结合中山大学附属第五医院的实践，介绍医院信息化网络设计与实现。阐明医院需求、网络设计整体情况、使用虚拟网的优势、工作站 IP 分配、VLAN 配置等方面的问题，并指出系统的应用实效。

〔关键词〕 医院；信息化；网络设计

**Network Design and Implementation of Hospital Informatization** *CAI Dong – jiang, Equipment Department, Fifth Affiliated Hospital of Sun Yat – Sen University, Zhuhai 519000, China; WU Ping – feng, Equipment Department, Peking University Shenzhen Hospital, Shenzhen 518035, China*

〔**Abstract**〕 Combining with the practice experiences of Fifth Affiliated Hospital of Sun Yat – Sen University, the paper introduces the design and implementation of hospital informatizatioon, elaborates the problems including the requirements of hospital, the whole design of the network, the advantages to applying virtual network, IP distribution in the workstation, VLAN configuration and so on, points out the application effectiveness of the system.

〔**Keywords**〕 Hospital; Informatization; Network design

## 1 医院需求

### 1.1 总体需求

医院的网络建设方案需要在满足各种信息传输的要求和适应未来网络发展之间寻求一个最佳的平衡点。中山大学附属第五医院是一家卫生部部属的综合性医院，医院希望通过应用网络技术增进科室之间的沟通、协调，提高工作效率，更好地服务病人，获得良好的社会效益和经济效益。由于医院承担着医疗、科研、预防和教学等各项任务，这就要求建立一个高速的园区网。作为高速园区网，首先应具有一定的先进性、良好的安全性、稳定性、易管理性和可扩展性。在有限投资条件制约下，实现网络的最佳应用，同时为将来网络进一步扩展及应用系统的发展、集成留有一定的余地。其次则要认识先进性和实用性的辩证关系，充分利用当今计算机与通讯技术的最新成果，保证系统有较长的生命周期，同时考虑医院的实际情况，把先进的技术和实用的产品融为一体[1]。此外所选产品应符合国际技术规范和标准，具有开放性，支持多种协议和多种接口及跨平台应用。

### 1.2 具体需求

1.2.1 *可靠性和高安全性* 一方面，网络技术给医院的医疗工作带来了便利，给病人提供更便捷、有效的服务。另一方面，要保护重要信息数据免受攻击或丢失。网络需要全天候不间断运行，不允许有网络中断的情况发生。医院的信息化建设对于安全性、可靠性的要求，可以说是重中之重。这就要求在设计之初必须把安全性、可靠性融合到网络基

〔修回日期〕 2010 – 12 – 17

〔作者简介〕 蔡东江，助理工程师，发表论文 8 篇。

础设施的每个部件，做到万无一失。

1.2.2 高带宽 医院广泛采用的信息化系统是 HIS 系统和 PACS 系统，为了满足日常的电子病历、远程诊断和会诊、临床教学需求，要求能实现信息化语音、医学图形、图像的获取、显示、存储、调用、处理和大量医学数据高速传输，其特点就是信息量极大，所以对网络的传输性能提出了更高的要求。

1.2.3 各个网段访问权限设置不同 目前很多医院组网中的 PC 和终端都处于对等机的地位，权限都一样，访问外部资源的权限也是一样的。这样就会给网络安全带来一定的隐患，也增加网络维护的难度。所以需要对不同职能部门的终端，设置不同的访问内网或外网的权限。

1.2.4 可管理性 网络的设计要方便将来网络管理人员的管理。同时要求交换机支持网络模块的热插拔，方便维护、检修，保证系统不间断持续运行。另外设备要能够支持 IEEE 802.1Q 协议，满足院内通过虚拟子网（VLAN）技术隔离的各部门网段之间流量的要求，针对不同的网络流量划分优先级别。

1.2.5 高扩展性 由于医院网络的重要性，使其可靠性、安全性、可管理性和可扩展性都受到了空前的重视。特别是网络的扩展性更是不同程度地影响着可靠性、管理性和安全性。良好的扩展性就意味着网络具备良好的持续改进能力。医院规模和业务的不断发展、接入用户数的不断增多、数据流量的不断加大都对网络提出扩展升级的需求[2]。所以在设计的时候应该充分考虑到网络的扩展性。

## 2 网络设计整体概况

### 2.1 核心设备

为满足医院的应用需要，全面提高医院的管理、医疗水平和整体素质，采用交换式以太网技术为网络解决方案，全网千兆骨干连接。考虑到网络的可扩展性和可靠性，配置两台大硬盘容量的数据库服务器和两台千兆路由交换机作为网络核心设备，两者之间分别做备份冗余链路，这样即使一个核心路由交换机或服务器因故障、软件升级或其它维护的需要而中断运行时，备份的冗余设备可以承担必要的服务以保证无中断的数据提供，保证设备应用的持续性，提高了网络的可靠性。同时位于网络中心的数据库服务器构成一个服务于全院业务工作的、快速的、分布式的数据库系统。

### 2.2 堆叠设计

在各栋大楼中同样用千兆交换机做汇聚层交换机，在接入层交换方面全面采用可扩充堆叠百兆交换机，100M 交换到桌面。交换机通过特殊设计的矩阵式堆叠模块 MSM，使得最多 7 个交换机可堆叠在一起，每个堆叠可形成多达 196 个 10/100M 端口容量。在堆叠中交换机之间的连接带宽为 2.1G，从而排除了传统的交换机通过 100M 双绞线串接而形成的瓶颈问题，每个堆叠的总体交换背板带宽为 16.8G，吞吐量为 5.6G，真正实现了扩充堆叠的设计。这样的堆叠设计与医院综合病房大楼结构化综合布线工程形成较好的配合，在网络方案设计中，只需根据不同楼层网络节点数的分布而采用不同数量的交换机堆叠，使得网络设计非常灵活方便，同时也方便以后网络的扩展。

### 2.3 拓扑设计

整体的拓扑设计采用核心、汇聚、接入 3 层架构，这使得不同层次设备能各司其职，对某一层次的网络设备进行升级改造，不会对其他层次的设备造成大的影响，这为网络故障定位、故障隔离以及网络可扩展性都带来了方便。在核心千兆交换机与各栋大楼主交换机之间，采用可靠、高速的千兆以太网络技术实现连接，以确保骨干网络的可靠性和高性能[3]。例如在住院部核心交换机通过千兆多模光纤分别连接到住院楼主交换机，在住院楼主交换机上配置 1 块 Switch Controller、1 块 8 口的千兆光纤模块、1 块 8 口的千兆 RJ－45 口模块，用来为各大楼主交换机提供千兆 Base－T 上链端口连接，再由住院楼主交换机通过千兆多模光纤连接到每楼层的交换机，根据各层信息点多少，选择交换机台数进行堆叠，最后通过 5 类双绞线连接上工作站，从而为桌面用户提供

10/100M 连接和交换能力，其他大楼的情况类似。中山大学附属第五医院网络结构，见图 1。

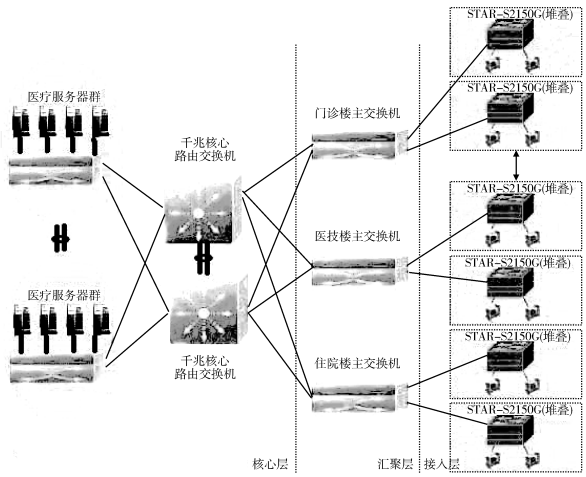


**图 1 中山大学附属第五医院网络结构**

在图 1 中，医疗服务器群里的服务器之间用千兆双绞线连接，服务器群之间、千兆核心路由交换机之间同样是用千兆双绞线连接，同时用双链路确保数据的正常传输；服务器群与千兆核心路由交换机之间、千兆核心路由交换机与各楼主交换机之间通讯用千兆多模光纤，并做备份冗余链路；主交换机到各堆叠用千兆多模光纤，最后通过百兆双绞线到终端，保证桌面网速满足日常工作要求。整个系统的网络平台根据医院的不同职能部门规划为若干个功能相对独立的局域子网，通过快速主干网互联，构成整个医院的网络拓扑。不同的工作站按不同的要求划分到许多不同的虚拟网中，这些工作站可以处在不同的物理局域子网上，但他们之间可以像在同一个局域网上那样自由通信而不受物理位置的限制。在这里网络的定义、划分与物理位置、物理连接是没有任何必然联系的。网络管理员可以根据不同的需要，通过相应的网络软件灵活地建立和配置虚拟网，并为每个虚拟网分配它所需要的带宽。有多种方式可以用来划分虚拟网，主要有根据端口定义、根据 MAC 地址定义、根据网络层定义和根据 IP 地址定义。

## 3 使用虚拟网的优势

### 3.1 减少潜在开销

选择虚拟网的主要原因就是虚拟网能够减少用户的增加、删除、移动等产生的潜在开销。在任何一种规模的网络中这笔开销都是不可低估的。能够支持虚拟网的交换机在没有路由器的情况下很好地控制广播流量。在虚拟网中服务器到客户端的广播信息只会在连接客户机的交换机端口上被复制，而其他端口上广播信息终止。只有那些需要跨越虚拟网的数据包才会穿过路由器。在这种工作方式下，交换机事实上扮演的是路由器的角色，有效地避免了网络堵塞。

### 3.2 建立虚拟工作组模型

虚拟工作组使用虚拟网的另一个目的是建立虚拟工作组模型。当虚拟网建成之后某一部门或分支结构的职员可以在虚拟工作组模式下共享同一个“局域网”。这样绝大多数的网络流量都限制在虚拟网广播域内部。当部门内的某一个成员移动到另一个网络位置上时，他所使用的工作站不需要做任何改动。相反一个用户不用移动他的工作站就可以调整到另一个部门去。虚拟网的这种功能使人们以前曾设想过的动态网络组织结构成为可能，并在一定程度上大大推动了交叉工作组的形成。

### 3.3 增加工作灵活性

医院经常会针对某一个科研项目临时组建一个由多个科室、部门的医疗专家组成的科研小组，有了虚拟网小组内的成员不用再集中到一个办公室里，只要坐在自己的计算机旁就可以了解到其他部门的研发情况。虚拟网带来了巨大的灵活性，当有实际需要时一个临时虚拟网可以应运而生。当项目结束后临时虚拟网又可以随之消失。这样无论是对用户还是对网络管理员来说都提供了不少便利。

### 3.4 实现网络管理有序化

医院的医疗信息、办公管理信息和财务管理信息基本上是分立的，没有必要将医疗方面的信息向所有的办公管理和财务管理工作站进行广播。可以控制将病人的基本资料和费用情况向指定的财务工作站开放，也可以将指定的办公管理工作站对所有的工作站进行广播。这样就可以实现整个网络管理的有序化和高效率，使网络运行在最佳状态。

## 4 工作站 IP 分配情况

用目前最常用的按端口划分 VLAN 的配置方法，给局域网 VLAN 进行配置，任何子网之间的通信都是通过 IP 地址来实现正确寻径。考虑到未来随着医院信息化的发展，预留足够多的网络端口以满足不断增加的需求。在第 3 层接入层上划分虚拟子网，规划 IP 子网，防止混乱和 IP 地址盗用。对医院的不同职能部门，根据具体使用的终端台数合理划分子网网络标识、IP 地址和子网掩码。具体划分，见表 1。

**表 1 中山大学附属第五医院各系统子网网络标识、IP 地址、子网掩码划分**

| 系统 | 台数 | 子网网络标识 | IP 地址 | 子网掩码 |
|---|---|---|---|---|
| 院长管理 | 10 | 192.168.2.0 | 192.168.2.1 – 254 | 255.255.255.0 |
| 医疗保险 | 10 | 192.168.3.0 | 192.168.3.1 – 254 | 255.255.255.0 |
| 财务科、挂号收费 | 50 | 192.168.4.0 | 192.168.4.1 – 254 | 255.255.255.0 |
| 人事管理 | 5 | 192.168.5.0 | 192.168.5.1 – 254 | 255.255.255.0 |
| 影像、检验资料管理 | 30 | 192.168.6.0 | 192.168.6.1 – 254 | 255.255.255.0 |
| 设备管理 | 5 | 192.168.7.0 | 192.168.7.1 – 254 | 255.255.255.0 |
| 行政、卫生耗材管理 | 10 | 192.168.8.0 | 192.168.8.1 – 254 | 255.255.255.0 |
| 药品管理 | 20 | 192.168.9.0 | 192.168.9.1 – 254 | 255.255.255.0 |
| 图书管理 | 50 | 192.168.10.0 | 192.168.10.1 – 254 | 255.255.255.0 |
| 医生医嘱 | 100 | 192.168.11.0 | 192.168.11.1 – 254 | 255.255.255.0 |
| 上 internet 网 | 100 | 192.168.12.0 | 192.168.12.1 – 254 | 255.255.255.0 |

对上述部门用户单独划分 VLAN，以确保相应部门网络资源安全。针对医院的网络拓扑结构，结合各部门计算机的分布情况，分别给 3 栋大楼配备一定数量的交换机，并且给其命名。门诊大楼配置交换机 6 台，分别命名为：Outp Switch1 – 6，医技大楼配置交换机 8 台，分别命名为：Tech Switch 1 – 8，住院大楼配置交换机 8 台，分别命名为：Inpa Switch 1 – 8。通过 VLAN 的划分，各系统对应的 VLAN 号、VLAN 组名及所对应的网段，见表 2。

**表 2 中山大学附属第五医院各网络系统 VLAN 号、VLAN 组名及网段**

| 系统 | VLAN 号 | VLAN 组名 | 台数 | 端口号 |
|---|---|---|---|---|
| 院长管理 | 2 | Manag | 10 | Outp Switch1 2 –11 |
| 医疗保险 | 3 | Insur | 10 | Outp Switch1 12 –21 |
| 财务科、挂号收费 | 4 | Treas | 40 | Outp Switch2 2 –21 |
| | | | | Outp Switch3 2 –21 |
| 人事管理 | 5 | Infor | 8 | Outp Switch4 2 –9 |
| 影像、检验资料管理 | 6 | Data | 30 | Tech Switch1 2 –21 |
| | | | | Tech Switch2 2 –11 |
| 设备管理 | 7 | Equip | 5 | Tech Switch2 12 –16 |
| 行政、卫生耗材管理 | 8 | Daily | 10 | Tech Switch3 2 –11 |
| 药品管理 | 9 | Medic | 20 | Tech Switch4 2 –21 |
| 图书管理 | 10 | Book | 50 | Tech Switch3 12 –21 |
| | | | | Tech Switch5 2 –21 |
| | | | | Tech Switch6 2 –21 |
| 医生医嘱 | 11 | Instr | 100 | Inpa Switch1 2 –21 |
| | | | | Inpa Switch2 2 –21 |
| | | | | Inpa Switch3 2 –21 |
| | | | | Inpa Switch4 2 –21 |
| | | | | Inpa Switch5 2 –21 |
| 上 internet 网 | 12 | Inter | 100 | Outp Switch5 2 –21 |
| | | | | Outp Switch6 2 –11 |
| | | | | Tech Switch7 2 –21 |
| | | | | Tech Switch8 2 –11 |
| | | | | Inpa Switch6 2 –21 |
| | | | | Inpa Switch7 2 –21 |
| | | | | Inpa Switch8 2 –6 |

## 5 VLAN 配置过程

配置过程简单地说只需两步，即为各 VLAN 组命名；把 VLAN 对应到相应的交换机端口。通过使用 Windows 系统自带的“超级终端”（Hypertrm）程序来进行设置。首先设置好超级终端，连接上要配置的交换机，配置交换机的 VLAN，连接成功后在主配置界面单击“K”按键进入命令行配置界面，在命令提示符下输入“enable”，进入特权模式。为

了安全和方便起见，分别给每个交换机命名，并且设置特权模式的登录密码。以 Outp Switch1 为例进行设置，代码如下：

```
(config)#hostname Outp Switch1
Outp Switch1(config)# enable password level 15 XXXXXX
Outp Switch1(config)#
```

设置 VLAN 名称，11 个 VLAN 分属于不同的交换机，故需要给不同的 VLAN 命名，按表 1 规则进行配置，如：Outp Switch1(config)# vlan 2 name Manag 等。把 VLAN 对应于表 2 所规定的交换机端口号。VLAN2、3、5 是分别在一个交换机上的，而 VLAN4、12 跨越了两个交换机，那么它们的配置不同，选择“Static”（静态）方式，对 VLAN2、3、5 的端口号进行配置。名为“Outp Switch1”交换机的 VLAN 端口号配置代码如下（包括两个 VLAN 组的配置，以 VLAN 2（Manag）为例）：

```
Outp Switch1(config)#int e0/2
Outp Switch1(config-if)#vlan-membership static 2
……
Outp Switch1(config-if)#int e0/11
Outp Switch1(config-if)#vlan-membership static 2
Outp Switch1(config-if)#
```

依此类推可完成 VLAN3、5 的端口号配置。由于 VLAN4、12 跨越两个交换机，这就必须配置主干（Trunk）来连接这些交换机。要求在这种主干链路上使用诸如 ISL 的主干协议，使用 Trunk 接口配置命令将一个快速以太网接口设置成主干模式，在交换机上有两个快速以太网接口 fa0/26 和 fb0/27。在使用动态交换链路协议（DISL）为 ISL 时，启用和定义主干协议类型可以静态或动态地进行。对于交换机（Outp Switch2），VLAN4 端口号的配置如下：

```
Outp Switch2#configure terminal
Outp Switch2(cofig)#vtp server domain VLAN4(将交换机设置为服务机)
Outp Switch2(config)#int e0/2
Outp Switch2(config-if)#vlan-membership static 4
……
Outp Switch2(config-if)#int e0/21
Outp Switch2(config-if)#vlan-membership static 4
Outp Switch2(config)#interface e fa 0/26
Outp Switch2(config-if)#trunk on
Outp Switch2(config-if)#vlan-membership static 4
Outp Switch2(config)#interface e fb 0/27
Outp Switch2(config-if)#trunk on
Outp Switch2(config-if)#vlan-membership static 4
```

完成定义后，为了验证配置可以在特权模式使用“show vlan”命令显示出刚才所做的配置，检查定义是否正确。接下来就要通过设置来实现各 VLAN 之间的通信，使用 RSM 实现 VLAN 之间的路由设置。对于门诊大楼放置了 6 部路由交换机，将路由交换机 Outp Switch1 的第 5 槽配上 RSM。各路由交换机之间通过引擎上的快速以太网上联端口相连。在 RSM 为每个 VLAN 建立相应的 VLAN Interface，实现各 VLAN 之间通过 RSM 进行通信，以门诊大楼的交换机为例，具体配置如下：

```
RSM Configuration
Outp Switch1 > (enable) session 5
Router > enable
Router#configure terminal
Enter configuration commands, one perline. End with CNTL/Z.
Router(config)#interface vlan 2
Router(config-if)#ip address 172.168.2.0 255.255.255.0
Router(config-if)#no shutdown
Router(config)#interface vlan 3
Router(config-if)#ip address 172.168.3.0 255.255.255.0
Router(config-if)#no shutdown
Router(config)#interface vlan 4
Router(config-if)#ip address 172.168.4.0 255.255.255.0
Router(config-if)#no shutdown
Router(config)#interface vlan 5
Router(config-if)#ip address 172.168.5.0 255.255.255.0
Router(config)#interface vlan 12
Router(config-if)#ip address 172.168.12.0 255.255.255.0
Router(config-if)#exit
Router(config)#^Z
Router#copy running-config startup-config
Building configuration...
OK
```

当在 VLAN 之间进行 RSM 路由配置时，将在 RSM 中创建多个虚拟接口。这些接口与管理域中配

置的每个 VLAN 均保持了映射关系。每个 VLAN 的虚拟接口都配置一个 IP 地址，与 VLAN 直接相连的主机配置 IP 地址一样。当 VLAN 中的其他设备希望与非本地的目标设备通信时，将会使用这一地址作为缺省网关。

## 6 网络系统应用实效

### 6.1 高带宽、高速度

医院的网络应用需要满足大量的数据传输要求，并且要保证高效，这对于网络的性能有很高的要求。从网络硬件上讲方案中的千兆主干、百兆交换到桌面已充分满足日常业务需求。网络中的交换机有端口聚合和线路聚合的功能，提高响应速度，另外在光纤千兆网卡的基础上将提供千兆铜线网卡，利用 5 类双绞线即可实现千兆速率[4]。双千兆网卡通过链路聚合技术也可使网络带宽加倍，真正解决传输瓶颈问题。同时为 HIS、PACS 等医院信息系统的顺利应用提供了坚实的网络保障。

### 6.2 高稳定性和可靠性

采用多种手段确保服务器工作不间断，与双交换核心相对应，配置双服务器，服务器中配置了有容错功能的服务器网卡连接核心交换机。利用网卡的特性两台服务器可以互为备份。另外每台服务器中的另外一块网卡还与辅助交换机相连接，在主干交换机之间形成互为备份的关系。此外核心交换机支持引擎冗余、交换机电源模块配置冗余，光纤/网线链路冗余等方式，保证线路或者设备出现单点故障时整个医院网络依然保持数据正常交换。

### 6.3 高安全性

建成的网络系统按照权限级别实施访问控制，通过网络监控和访问控制可实现对各种网络病毒和黑客攻击行为的有效防范。先进的 802.1X 认证功能可对网络多种元素进行绑定，有效保障了接入用户的唯一性。在多种安全技术的支持下该网络完全保障了用户的信息安全。

### 6.4 高扩展性

核心交换机可为网络提供足够的弹性扩展功能，在未来可以非常方便地升级到万兆主干，同时该系列提供了领先的交换背板，不仅轻松满足了目前所有模块的线速转发，而且为新一代更高密度和复杂功能模块的应用提供硬件基础。主管理模块执行路由管理、网络管理、网络服务等任务，用户接口模块可以独立实现路由、交换、ACL、QOS 等功能，分布式处理设计极大地提高整机处理能力[5]。为未来网络扩展提供一定的空间，不但保护了现有用户投资，更避免了未来网络扩展在骨干设备上的重复投资。

### 6.5 管理更灵活

网络采用千兆以太网，主干和各网段及桌面能够实现无缝结合，网络管理变得简单。网络中的全部产品均支持统一的网管系统，提高了工作效率。网络管理软件通过提供设备管理图、拓扑状态图、流量分析图以及网络节点监控，将网络管理工作量降到最低，并可通过矢量图的形式进行远程查看。当发生网络故障的时候系统还可以自动向网络管理员发出报警信号。全中文菜单或图形配置方式为交换机的管理和配置提供了极大的便利。

## 参考文献


1 张立云，马皓，孙辨华. 计算机网络基础教程〔M〕. 第 1 版. 北京：清华大学出版社，2003，4.

2 Cisco System 公司. 思科网络技术学院教程（第一、二学期）〔M〕. 第 3 版. 北京：人民邮电出版社，2004.

3 张立云，邵武军，张红雨. 计算机网络基础教程〔M〕. 第 1 版. 北京：电子工业出版社，2000，8.

4 Michael Palner，Robert Bruce Sinclair 著，杨继萍，黄开枝译. 局域网与广域网设计与实现〔M〕. 第 1 版. 北京：清华大学出版社，2003.

5 Cisco System 公司. 思科网络技术学院教程（第三、四学期）〔M〕. 第 3 版. 北京：人民邮电出版社，2004.