文章编号：2095-2163(2021)02-0040-05 中图分类号：TP393.18 文献标志码：A

医院数据中心建设中网络规划研究与应用

吴冠朋
（山东省立第三医院，济南 250031）

摘 要： 随着医院数据中心建设愈发成为医院信息化建设的重要组成部分，网络建设作为数据中心建设的基础。本文以山东省立第三医院数据中心建设为例，介绍数据中心的网络规划和实施。文中网络建设划分为医院内网、医院外网两个区域。院内网区域实现医院 HIS、LIS、PACS 等主要业务安全稳定地运行，同时部署安全防护区域用于保护网络安全和数据安全。医院外网区域主要实现提供以面向患者服务的信息系统，同时部署安全产品进行互联网访问保护。通过网闸实现医院内网和外网区域的数据交换，本院数据中心网络规划与实施确保了网络通信与安全稳定运行，为数据中心提供了良好的网络基础。

关键词： 数据中心；信息系统；网络规划；网络通信

Research and application of network planning in hospital data center

WU Guanpeng
(Shandong Provincial Third Hospital, Cheeloo College of Medicine, Jinan 250031, China)

【Abstract】 With the development of hospital data center, its design has become an important part of hospital information construction. Taking the data center construction of Shandong Provincial Third Hospital as an example, the paper researches the network planning and implementation of the data center. The network construction is divided into hospital intranet and hospital extranet. The main business, such as HIS, LIS and PACS can run safely and stably in the hospital intranet area. At the same time, the security zone is deployed to protect network security and data security. The external network area of the hospital mainly provides patient oriented information system. After that, security products are deployed for Internet access protection. Data exchange between intranet and extranet in hospital is realized through gateway. The data center network planning and implementation in the hospital ensure the network communication and safe and stable operation. It provides a good network foundation for the data center.

【Key words】 data center; information system; network planning; network communication

0 引 言

随着信息化发展，国家加大基础建设投入，数据中心[1-3]建设成为政企、医院、学校等建设的重要组成部分。而数据中心建设包含硬件设备和软件设备。其中，硬件设备包含网络设备、服务器设备、安全设备等。而网络架构[4-5]作为数据中心的通信基础，也是建设数据中心必不可少的关键建设。本文以山东省立第三医院数据中心建设为例，介绍数据中心的网络规划和实施。本次研究的网络规划与实施很好地确保了网络通信与安全稳定运行。对此拟展开研究详述如下。

1 数据中心网络建设方案

医院数据中心的建设是医院信息化[6]建设的重要评判标准，数据中心建设需要合理规划数据中心网络架构、安全防范[7]体系建设、服务器集群搭建等。本文通过合理选用设备厂商提供的通信设备、安全交互设备、服务器等。数据中心网络建设方案如图 1 所示。图 1 中，数据中心区域主要是以服务器区域为主，包含院区的医院信息系统（Hospital Information System，HIS）、实验室信息管理系统（Laboratory Information Management System，LIS）、医学影像存档与通讯系统（Picture archiving and communication systems，PACS）、电子病历系统（Electronic Medical Record，EMR）等，是医院业务展开的核心。其次，是运维管理区域，包含运维管理系统、认证系统等。安全防护区域包含：准入系统、杀毒系统、日志审计系统、数据库审计系统、堡垒机系统、VPN 接入系统等。院区网主要分为医院内网和医院外网，都是通过标准三层网络架构，包含核心设备、汇聚设备、接入设备等。院区内外网络通过具有网络隔离的网闸设备进行内外网间的数据交互。对外网区域包括互联网出口防火墙、上网行为管理系统等进行网络保护与行为管理。

作者简介：吴冠朋（1989-），男，硕士，山东省立第三医院信息网络部工程师，主要研究方向：人工智能与图像处理技术。
通讯作者：吴冠朋 Email：zbxywgp@163.com

收稿日期：2020-11-18

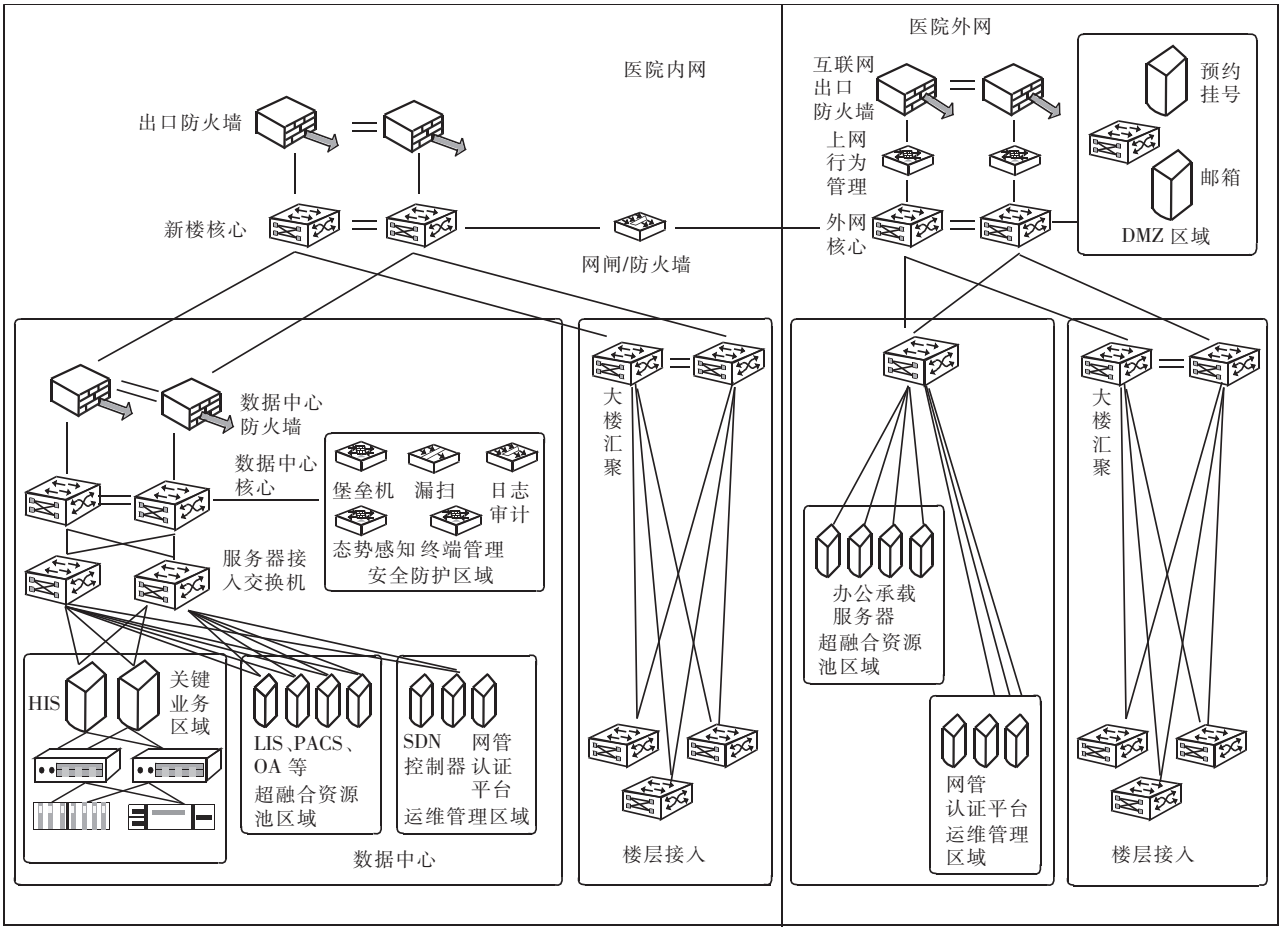

图 1　数据中心网络架构图

Fig. 1　The network framework of data center

2　数据中心网络架构规划与实施

网络架构的规划与实施是数据中心建设的基础，为达到网络架构规划与实施，对此可做阐释分述如下。

2.1　数据中心建设需求

以网络应用需求、网络性能需求、信息点统计作为网络规划需求分析。网络应用应满足目前院区现有 HIS 系统、LIS 系统、PACS 系统等业务，系统总体需要使用 HTTP、FTP、HTTPS 等端口应用需求，核心层网络需要具备：整机交换容量≥150 Tbps，包转发率≥36 000 Mpps，业务插槽数量≥6，全宽主控引擎槽位≥2，独立交换网板槽位≥1 个等。汇聚层设备需要满足：交换容量≥23 Tbps，包转发率≥1 080 Mpps，万兆光接口≥48，40 G 光接口≥2 等。接入层设备需要满足的性能：千兆电口≥48 个，万兆光接口≥2 个，万兆电口≥2 个；整机交换容量≥330 Gbps，转发性能≥160 Mpps 等。并且所有网络设备可以做到物理设备虚拟化、支持冗余链路。信息点统计主要是以电脑、打印机等接入终端数量，信息点达到 2 000 多，根据楼宇及楼层划分不同的虚拟局域网（Virtual Local Area Network，VLAN）。实现网络的访问隔离。

2.2　综合布线[8-9]总体设计

根据院区现有 HIS 系统、LIS 系统、PACS 系统等业务，结合网络总体设计考虑到楼宇间、中心机房的综合布线[8]、楼宇间互联设备及传输介质的选择、主干链路带宽、接入带宽、无线网络方案等多种需求。楼宇间、中心机房的综合布线以支持万兆传输的 6 类双绞线及支持万兆光纤作为主要布线方式。楼宇间互联设备通过长距离的万兆光纤进行互联，为了保证链路传输的稳定性及安全性，楼宇互联设备采用双冗余链路。主干链路带宽通过 4 台核心设备两两形成虚拟化，主干链路之间通过 4 条 10 G 链路聚合成一条 40 G 逻辑链路，增加链路带宽、提高网络安全性等。接入带宽主要是以满足临床对 PACS 系统的需求，接入电脑支持千兆链路接入。为满足移动护理、手持终端 PDA 的需求，无线网络同样采用标准化三层网络架构，且通过安全加密认证方式达到内网访问的安全性。例如诊室的设计图

纸，见图 2。图 2 中，TN 表示内网接入点。

2.3 网络三层结构设计。

数据中心网络建设采用标准三层架构，详见图 3。由图 3 可知，该架构包含核心层、汇聚层、接入层架构。根据接入信息点的数量计算出接入层设备、汇聚层设备、核心层设备的数据交换率、转发率、路由条数目、ARP 数量、路由方式、负载分担、虚拟化等功能。

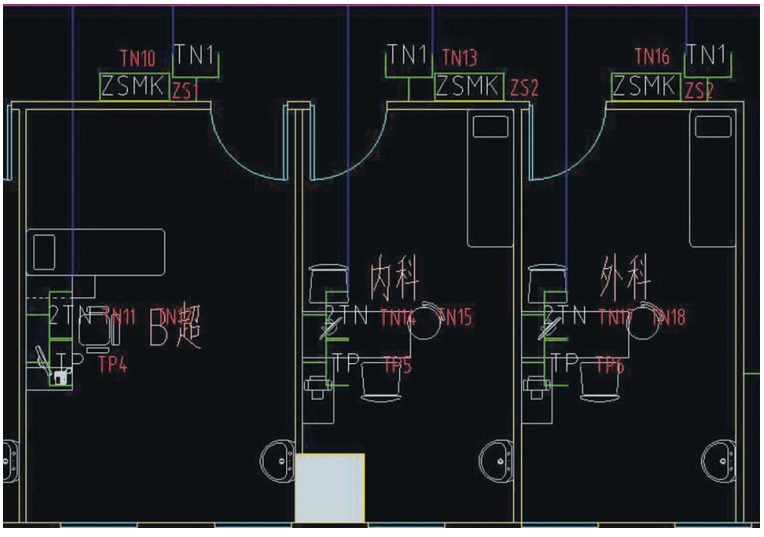

图 2 网络综合布线

Fig. 2 Network generic cabling

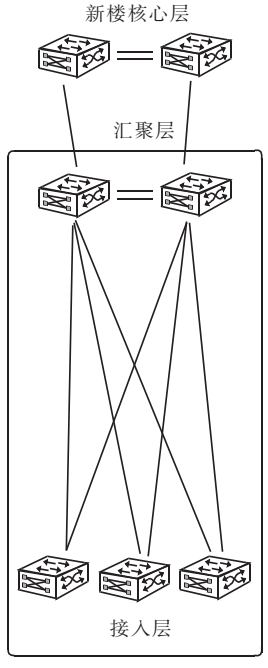

图 3 3 层标准网络架构

Fig. 3 Three layer standard network architecture

核心层设备采用 2 台 H3C 的 7506E 作为核心交换机，并且通过其独有的智能弹性框架技术（Intelligent Resilient Framework，IRF）将设备上多台物理接口连接在一起后通过 IRF 技术将多台物理设备虚拟成一台逻辑设备。在设备上完成虚拟化后的配置如图 4 所示。

```
<JTYY_CS-S7506E-V>dis irf
MemberID  Slot  Role    Priority  CPU-Mac         Description
 *+1      0     Master  1         00e0-fc0a-15e0  -----
   2      0     Slave   2         00e0-fc0f-8c13  -----
--------------------------------------------------
```

图 4 核心交换机上的虚拟化配置

Fig. 4 Virtualization configuration on core switch

在核心交换机上完成业务接入虚拟局域网[10]（Virtual Local Area Network，VLAN）设计、物理接口链路聚合、访问控制策略、流量镜像、访问路由、登录方式等。

汇聚层设备主要完成接入层设备的汇聚、流量转发、网络隔离、协议过滤等功能。汇聚层设备采用 2 台 H3C 的 S6520 作为汇聚交换机，同样通过 IRF 技术实现物理设备虚拟化，并且在上行链路连接至汇聚交换机时采用冗余口字型链路，提高网络稳定性，降低因单链路、单点故障而导致的网络中断，汇聚交换机上物理接口上的配置如图 5 所示。

```
irf-port 1/2
 port group interface Ten-GigabitEthernet1/0/47
 port group interface Ten-GigabitEthernet1/0/48
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/0/47
 port group interface Ten-GigabitEthernet2/0/48
#
interface Bridge-Aggregation1
 description 1kou-juhe
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 101
 link-aggregation mode dynamic
#
interface Bridge-Aggregation2
 description 2kou-juhe
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 102
 link-aggregation mode dynamic
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 description 1kou-juhe
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 101
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 description 2kou-juhe
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 102
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 description 3kou-juhe
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 103
 port link-aggregation group 3
```

图 5 汇聚交换机虚拟化及物理接口配置

Fig. 5 Virtualization and physical interface configuration of aggregation switch

接入层交换机主要完成终端设备的接入，通过在不同楼层划分不同的 VLAN，实现网络访问隔离。并且接入层交换机通过链路聚合分别上联不通的 2 台汇聚交换机，实现物理链路的冗余。接入交换机上的聚合链路及接入 VLAN 如图 6 所示。

```
#
interface Ten-GigabitEthernet1/0/49
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 103
 port link-aggregation group 49
#
interface Ten-GigabitEthernet1/0/50
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 103
 port link-aggregation group 49
#
interface Ten-GigabitEthernet2/0/49
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 103
 port link-aggregation group 49
#
interface Ten-GigabitEthernet2/0/50
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 17 103
 port link-aggregation group 49
#

 interface GigabitEthernet2/0/1
  port access vlan 103
  stp edged-port
 #
 interface GigabitEthernet2/0/2
  port access vlan 103
  stp edged-port
 #
 interface GigabitEthernet2/0/3
  port access vlan 103
  stp edged-port
 #
 interface GigabitEthernet2/0/4
  port access vlan 103
  stp edged-port
 #
 interface GigabitEthernet2/0/5
  port access vlan 103
  stp edged-port
 #
 interface GigabitEthernet2/0/6
  port access vlan 103
  stp edged-port
```

图 6　接入交换机上的聚合链路及接入 VLAN

Fig. 6　Aggregation link and access VLAN on access switch

以部分楼层 IP 及网络划分为例，具体规划见表 1。

表 1　VLAN 与 IP 地址规划

Tab. 1　VLAN and IP address planning

楼层/层	VLAN ID	IP 地址/掩码	网关
B2	VLAN 99	172.16.99.X/24	172.16.99.254
B1	VLAN 98	172.16.98. X/24	172.16.98.254
1	VLAN 101	172.16.101.X/24	172.16.101.254
2	VLAN 102	172.16.102.X/24	172.16.102.254
3	VLAN 103	172.16.103.X/24	172.16.103.254
4	VLAN 104	172.16.104.X/24	172.16.104.254
5	VLAN 105	172.16.105.X/24	172.16.105.254

3　安全防范体系建设

安全防范体系[11-12]建设分为内外网数据交互、互联网访问交互、院内安全管理区域。对此可给出探讨论述如下。

内外网数据的交互主要以网闸设备进行数据交换，网闸主要分为安全区域和非安全区，通常内网设备所在的区域为安全区，互联网设备所在的区域是非安全区。信息交互的原理是分时使用 2 个区域中的数据通道进行数据交换，类似船只摆渡原理。网闸能够在数据交换过程中进行恶意病毒攻击防范、恶意信息过滤，提高信息的安全性。

互联网访问交互主要是以防火墙设备为主，出口防火墙上配置双机冗余实现热备，这样一台设备故障其他设备接替工作，同时增强网络稳定性，保证业务的连续性。出口防火墙外网区域连接不同运营商线路，实现负载均衡的同时提高出口稳定性。互联网访问交互区域还部署 IPS 设备、WAF 设备、上网行为设备、终端准入与管理设备等安全产品。

院内安全管理区域主要是将安全设备通过旁路方式接入院内网络，安全设备包含 VPN、堡垒机、日志审计、数据库审计、终端准入、入侵检测等。通过 VPN、堡垒机、终端准入、入侵检测等安全设备的访问控制手段保护终端设备访问服务器；日志审计、数据库审计设备提供访问记录与操作记录，实现安全事件发生后的追踪。

4　结束语

本文中网络建设划分为医院内网、医院外网两个区域。内网区域建设可实现医院 HIS、LIS、PACS 等主要业务的安全稳定运行，同时部署安全防护区域用于保护网络安全和数据安全。医院外网区域主要提供面向患者服务的信息系统，通过网闸进行医院内网和外网区域的数据交换，实现面向患者服务的信息系统，同时部署安全产品进行互联网访问保护。目前，本院的网络规划与实施很好地确保了网络通信与安全稳定运行。今后将继续针对数据中心加强访问控制策略，进一步完善网络体系架构，提高数据安全性。

参考文献

[1] CAI Jun, ZHANG Zhuo , JI Zhengnan . Construction of data centre in campus network [C]// 2012 Second International Conference on Business Computing & Global Informatization. Shanghai, China:IEEE Computer Society, 2012:622-624.

[2] 魏祥麟, 陈鸣, 范建华,等. 数据中心网络的体系结构[J]. 软件学报, 2013(2):295-316.

[3] 许鑫, 苏新宁, 吴乃冈. 高校共享数据中心平台的设计与实现[J]. 现代图书情报技术, 2005(6):48-53.

（下转第 49 页）