医疗云网络构建及其安全方案研究

银 琳 范年丰 凌 翔

（中山大学附属第三医院信息科 广州 510630）

〔摘要〕 以中山大学附属第三医院为例，对比传统架构与医疗云网络架构不同之处，阐述医院云平台网络设计方案以及网络环境安全策略，指出云平台建设既有助于院内业务系统高效稳定运行，也可提升资源利用率。

〔关键词〕 医疗云；网络架构；虚拟化

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2019.03.006

Building of Medical Cloud Network and Study of Its Security Scheme *YIN Lin, FAN Nianfeng, LING Xiang, Information Department, the Third Affiliated Hospital of SUN Yat－sen University, Guangzhou 510630, China*

〔**Abstract**〕 The paper, by taking the Third Affiliated Hospital of SUN Yat－sen University as an example, contrasts the architecture of the medical cloud network with traditional architecture. It elaborates on the design scheme of cloud network in hospital and network environment security strategy, points out that building such a cloud platform will not only facilitate the effective and stable operation of service system in the hospital, but also improve the utilization rate of resources.

〔**Keywords**〕 medical cloud; network architecture; virtualization

1 引言

随着云计算技术的日渐成熟与普及，一些具有多年信息化基础的大中型医院根据自身信息化建设的发展规划，逐步将应用系统迁移到云平台[1]。中山大学附属第三医院是国家卫健委部属直管的综合性三级甲等医院，在广州分两个院区，随着医院信息化建设的不断深入，业务系统的不断上线和完善，医院数据中心建设面临诸多问题，如系统需求响应慢、硬件设备不断增加、IT 建设成本较高、运维压力日渐增大、院区分散管理困难、数据孤岛难以共享等[2]。医院与专业云的服务商合作，正逐步建立专有信息化云平台。而医疗云中的网络建设更是保证系统稳定安全运行的基石。本文通过医疗云在医院的逐步实施，探讨医疗云网络及其安全设计方案的可行性。

2 新旧网络拓扑架构对比

2.1 旧网络架构

医院旧网络架构是传统的业务网和外网完全物理隔绝，内外网架构各自都有核心、汇聚、接入3层。内网核心交换机为 CiscoNexus7010，采取双机热备份路由协议（Hot Standby Router Protocol，HSRP）模式；终端分别通过接入交换机接入内网访问网络资源，其网络拓扑，见图1。医院外网主要提供因特网访问，通过防火墙进行策略访问控制，仅部署网闸、防火墙、流量防御系统、防病毒设备以及流量控制设备等安全设备。传统的网络架

〔修回日期〕 2018－10－15

〔作者简介〕 银琳，中级工程师，发表论文4篇；通讯作者：范年丰，助理工程师。

构存在许多问题。在网络安全方面缺乏完善的安全防护措施及数据安全保障。网络中无安全准入系统，存在终端安全隐患。在网络拓扑结构方面，网络可拓展性差，主交换机双机热备，切换过程复杂。在网络硬件方面，设备使用年限长，性能不稳定，故障多发且无自动化运维工具。

2.2 基于医疗云的新网络架构

2.2.1 架构图 医院信息化建设需从实际需求出发，降低成本增加效益；以行业要求为标准，遵从规范；以成熟稳定为原则，适当超前，充分利用云技术来解决传统网络架构存在的问题。首先，根据医院业务需求对应于医疗云平台的实际配置和资源需求情况，拟构建两地三中心的框架，包括一个生产中心（在广州市内），一个异地灾备中心（除广州市外的广东省其他城市内），改造本地中心机房的数据中心作为应急灾备机房（全量业务系统），拟在云平台失效特殊情况下半小时内能够临时接管医院全量业务系统，保证医院信息系统（Hospital Information System，HIS）不中断，通过数据库同步技术保障业务数据与云平台的完整性和一致性，以实现主备容灾。医疗云网络架构，见图 2。

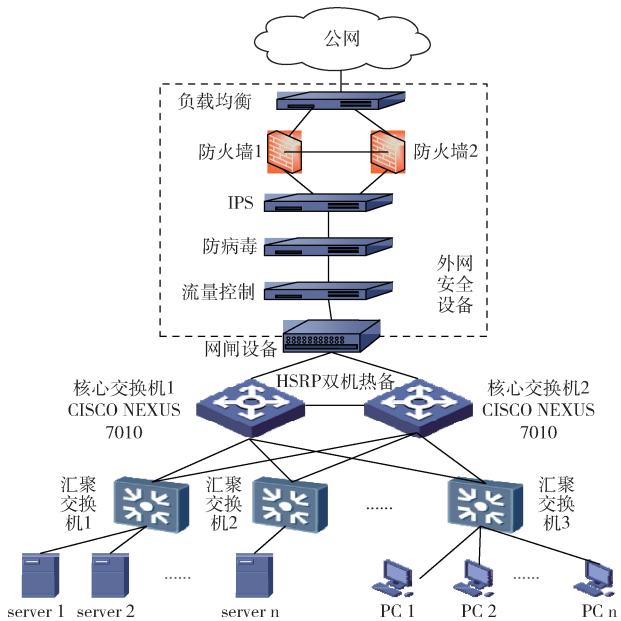

图 1 医院旧网络拓扑

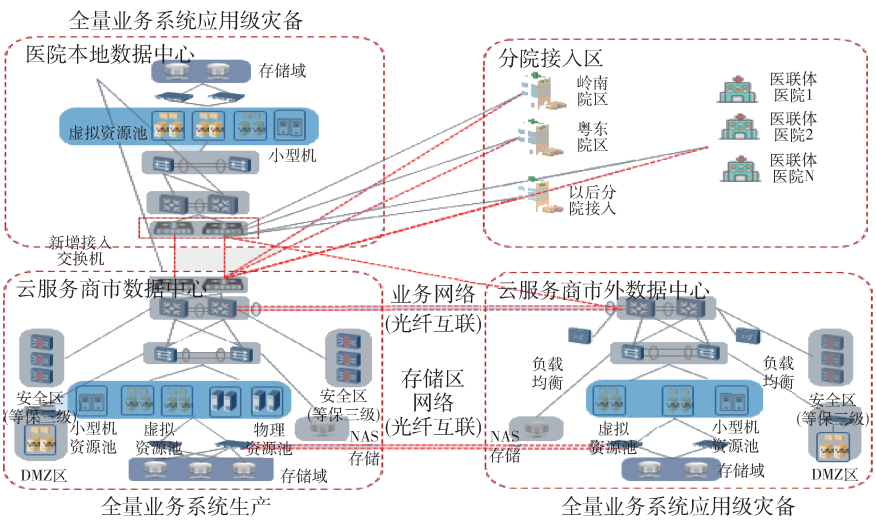

图 2 医疗云网络架构

2.2.2 架构分析 首先医院本地数据中心通过 1 条光纤链路和 1 条 1GB 的多业务传送平台（Multi Service Transfer Platform，MSTP）专线将完全不同的物理路径和云服务商市内异地数据中心互联，同时对原核心交换机做虚拟化改造，实现两条电路捆绑聚合，两条电路互为主备，相互负载。医院核心交换机的专线端口从两层到云平台的虚拟可扩展局域网（Virtual Extensible Local Area Network，VXLAN），再由 VXLAN 连接云平台，云端主机使用的 IP 地址段的网关设置在医院本地或者云端。由于整体网络采用大两层的方式，不会引起 IP 地址的冲突问题，且医院业务达到安全隔离的目标，另外在本地机房新增两台接入交换机，对外连接均接入交换机互联，分担核心压力，且有利于后续拓展。其次

医院本地数据中心通过 1 条 1G MSTP 专线和云服务商省内市外异地数据中心互联作为灾备使用。再次分院区各通过 1 条 500M MSTP 专线和云服务商市内异地数据中心互联作为灾备使用。

3 医院云平台网络设计方案

3.1 概述

针对目标与需求，医疗云平台网络建设通过租用云服务商的专网链路的方法组建医疗业务网络，根据业务需求弹性增加。医疗云的网络整体设计方案研究内容分为医院和云服务商数据中心内部的业务网络，医院内部的业务网络结构以及网络层的安全策略 3 部分。

3.2 医院和云服务商之间数据中心网络结构及涉及技术

医院和云服务商之间的网络连接由两条不同物理路由专线接入生产中心，同时 1 条专线接入灾备数据中心，3 条专线的冗余保护物理路径的光纤链路承载，直达云平台核心交换机，避免经过不安全的互联网，专网专用最大程度上保证医院通信安全。这 3 条专线采用链路聚合的方式实现互为主备、相互负载，从而提高链路的高可靠性和利用效率。数据中心之间的网络需要实现数据的高速互联同步，双链路且互为灾备。由于要达到双活数据中心，同一个业务通常会在两个数据同时部署，这时数据中心间需要两层互联。在业务迁移期间，为保证业务连续性需建立跨中心的服务器集群，构建跨越中心的两层互联网络实现服务器平滑迁移。结合医院业务需求，首选基于裸光纤的虚拟化技术，其次选择 L2GRE 互联。采用裸光纤快速切换的两层互联技术，在核心交换机上开启远程虚拟化实现 200 毫秒的快速切换。

3.3 医院内部业务网络结构及涉及技术

医院内部工作站之间采用光纤互连，工作站和网络之间通过多网络、多链路技术保证应用系统的计算和交换带宽。医院内部网络需具备高吞吐量和高可扩展的能力，也是满足医疗云平台后期业务增长的需要。内网所有网络设备、服务器网卡和连接需采用冗余架构，任意网络设备或链路故障不影响业务使用；每台虚拟化服务器需配置万兆接口用于南北流量访问（外部访问业务系统）；虚拟化服务器连接网络采用虚拟局域网（Virtual Local Area Netwrok，VLAN）隔离，上联端口启用 Trunk；连接虚拟化服务器的物理交换机 MTU 调整为 1 600；全网需启用动态路由协议，以适应虚拟化网络创建[3-4]；另外网络功能需减少对单一设备提供商的功能依赖，构建通用化网络架构。本方案拟利用网络虚拟化软件重新设计虚拟机网络，在原有的物理 VLAN 上构建全新的 VXLAN，为每套业务系统创建独立隔离网络，且多层应用架构中每个应用也应具备独立网络。医疗云平台利用与网络虚拟化管理程序的功能可在软件中重现第 2 ~ 7 层的整套网络服务（如交换、路由、访问控制、防火墙、QoS 和负载平衡）。可通过编程方式任意组合这些服务与策略，经过数秒的设置即可生成独一无二的隔离式虚拟网络，从而轻松快捷地实现主机和主机之间、相对独立应用系统之间、租用单位之间的横向隔离和访问控制。VXLAN 原则上可提供上万个隔离子网，满足细粒度隔离及医院系统应用需求，如医院财务核算、仓库管理、后勤管理系统等，与医院业务系统相对独立时需构建独立子网，仅授权财务部、仓管部、后勤部门等各自局域网内部访问权限。其次全新的 VXLAN 网络不仅实现每套业务系统均具备最小广播域，还可以避免广播风暴风险；同时利用网络虚拟化平台的分布式路由功能实现流量的最短路径，提高访问效率。最后结合边界网关服务可实现客户端到服务器端的网络访问控制，利用分布式防火墙完成单业务系统内部之间的访问控制。

3.4 网络环境安全策略

3.4.1 概述 利用路由器、交换机和相关网络设备建成，用于在本地或远程传输数据的网络环境中，在安全策略中，网络层中进行的各类传输活动的安全都应加以关注[5]。现有的大部分攻击行为包括病毒、蠕虫、远程溢出、口令猜测等都可以通过网络实现。网络层主要考虑的技术包括结构安全与网段划分、网络访问控制、网络安全审计、边界完

整性检查、网络入侵防范等[6]。

3.4.2 DMZ 网络链接区设立 医院核心交换机的专线端口由 VXLAN 网络连接医疗云平台，云端主机使用的 IP 地址段的网关设置在医院本地。由于整体网络采用大两层的设计方式，不会引起 IP 地址的冲突问题，从而医院的业务不允许外部访问，达到安全隔离的目的。但医院部分业务系统需要访问公网，因此在医疗云资源池专门设置非军事区（Demilitarized Zone，DMZ）网络链接区，将医院 Web、Mail、文件传输协议（File Transfer Protocol，FTP）等允许外部访问的端口单独接在该区端口，使整个需要保护的内部网络接在信任区端口，不允许外部访问，实现内外网分离，达到安全要求。

3.4.3 访问控制设计 在医院云网络各区域边界中，采用边界访问控制技术，防止未授权访问发生。通过防火墙设备和 VLAN 划分配置予以实现。根据医院网络的实践情况，在互联网出口区域边界利用防火墙设备的入侵防护实现各区域之间的访问控制，而对于其他医院物理区域内部的不同网段之间的边界，则采用 VLAN 划分结合访问控制列表（Access Control List，ACL）的方法予以隔离。

3.4.4 带宽管理 医院信息系统设定网络带宽策略。对于医院重点业务系统的应用或协议应分配更多的带宽资源；针对辅助业务应用，可限制其流量，以保证重点业务的可用性，也可以通过限制协议的方式保证主要协议的可用性。带宽管理可利用专业的流量管理设备或网络设备的服务质量（Quality of Service，QOS）策略配置来实现。

3.4.5 网络入侵防范 医院网络安全的重要保证，其提供主动实时的防护，对医院信息系统连接和访问的合法性进行控制，监测网络攻击事件等，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是简单地在监测到恶意流量时或之后才发出告警，满足医院 24 小时网络安全要求。一方面，网络入侵保护系统检测到医院内部业务网络接收到恶意数据流量时会自动地将攻击包丢掉或采取措施将攻击源阻断，而不是将攻击流量放进内部网络导致业务系统缓慢；另一方面，入侵检测系统的部署可将医院信息系统内部交互的流量镜像到网络入侵检测系统，可随时监测医院信息系统的流量是否异常。

3.4.6 网络安全审计 监控网络边界中进出的内容和已授权的正常内部网络访问行为，可通过安全审计系统的部署来解决。通过连接云平台上的安全审计系统实现对服务器区域访问的全面细粒度审计。审计内容包括 FTP、TELNET、SMTP、POP3、数据库访问、运维人员运维过程等，这样在遇到紧急事件后可以有效追查和问责。

4 结语

本方案以统一的技术架构为约束，采用适度超前的技术，如网络虚拟化、访问网络监控平台等，根据医院业务平台特点，分类规划设计医院业务平台面向两地 3 中心的部署模式。医院医疗云的网络架构在不断修正中已基本构建完成，其安全策略正在逐步实施过程中。此模式为实现更高的资源利用率，更短的业务中断时间，更好的恢复点目标（Recovery Point Objective，RPO）和恢复时间目标（Recovery Time Objective，RTO），更加敏捷的业务部署以及自动化的容灾流程等提供可能。但同时值得注意的是方案需根据医院自身业务多场景的需求合理规划云服务内容，尽量采用松耦合架构，不要片面追求上云带来的成本下降，需从长远运营角度来核算成本。

参考文献

1 陈佳阳，王林蕾. 云计算与智慧医疗系统建设［J］. 信息系统工程，2018，2（1）：27.

2 翁锦阳，朱铁兵. 大型医院基础设施私有云的设计和应用［J］. 中国卫生信息管理，2015，6（4）：607－609.

3 王纯子，张斌，李艳. 云网络安全技术研究现状综述［J］. 信息技术与信息化，2015，8（2）：21－22.

4 王春容，曾宇平. 医院虚拟化云平台构建研究［J］. 医学信息学杂志，2016，37（5）：24－27.

5 董飞宇. 云网络安全技术浅析［J］. 信息技术与信息化，2017，8（2）：87－88.

6 蒙华，刘德健，张冰，等. 基于第三方医疗云环境的医疗大数据安全探讨［J］. 中国数字医学，2018，3（3）：23－25.