示，确保安全防护紧跟业务，无论 VM 飘到那个物理节点，虚拟安全资源都能为其提供防护。

3　统一运维监控平台

由于医院网络规模不断扩大,设备数量增多,网络协议的多样化,跨区域协作难度大,这给医院网络运维人员的日常工作带来了巨大挑战。为了有效提升医院网络运维监控工作，极大程度地帮助运维人员发现问题，定位问题，解决问题和问题溯源，需要建设一套跨多个数据中心的统一运维监控平台,方便运维人员在一个院区监控整个医院的网络运行情况。此外，在传统的数据中心的模式下，数据流量主要是由终端通过接入、汇聚、核心至服务器进行数据交互的南北方向。而集团化医院的多数据中心,不仅有南北流量,还将产生虚拟机之间、数据中心之间的东西向流量。因此，多数据中心的管理平台还需要重点关注东西向的带宽利用率，并发数等。

统一的网管监控平台的建设规划不仅要实现传统的网络监控,还需要针对临床医疗的业务特点，统计、分析临床使用的业务波动，深挖网络与服务的潜在问题。监控平台主要涵盖动环监控、网络与服务、网络性能、虚拟机性能和业务监控等五大内容，如图 4 所示。

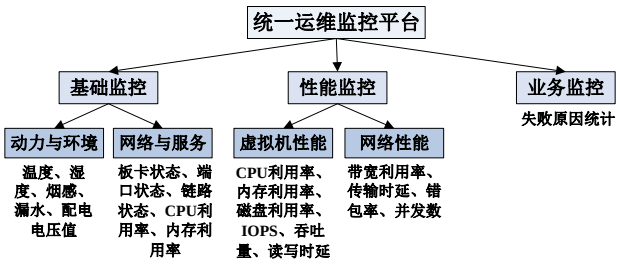

图 4 统一运维监控平台的指标体系

网络性能需要制定相应指标的阈值。例如，当带宽利用率超过 80%时，可能发生数据包拥塞的情况，存在丢包重传的隐患；当跨院区传输时延大于 5 毫秒时，将会影响数据中心间的同步，需考虑切换备用线路。

虚拟机性能不仅仅需要观察 CPU 利用率，内存利用率，更需要关注 IOPS（Input/Output Operations Per Second，IOPS），读写延迟，吞吐量等。服务器节点的读写速度将直接影响到医生查询报告，护士刷系统领药单等查询响应时长，关系到临床对信息系统使用的满意度。对于 IOPS 量较大的虚拟机可迁移至全闪存节点提高读写效率；对于吞吐量较高的虚拟机可增加 CPU、带宽等资源。

由于在医院运行过程中，常常出现收费处支付异常情况，医院信息系统（Hospital Information System， HIS）调用第三方接口失败等情况。为此，笔者认为医院今后的监控平台不仅要关注网络、服务器等基础设备，更需要关注上层业务应用情况。通过读取系统日志，统计医保、银联支付失败或“单边账”的错误值（error code）或原因值（cause code）；统计 HIS 与影像系统（Picture Archiving and Communication Systems，PACS）等接口调用时系统响应异常的原因等。通过平台搜集、统计和分析医院业务使用层面的异常情况，帮助运维人员挖掘网络和服务的潜在问题。

4　结语

本文思考通过环形的双冗余传输架构构建多区域数据中心,增加通信稳定性。采用 VxLAN 技术实现跨院区的大二层网络互通，保证医疗业务的连续性。建设统一的运维监控平台，提升多数据中心的运维效率。

集团化医院下，多院区数据中心将融为一张整体的网络。在方便医院统一运营和管理的同时，也给医院的网络安全埋下了潜在的隐患。一旦单个院区遭受安全威胁，势必将影响整个医院下多个院区的网络安全态势。此外，动态的业务均衡也使得医院安全防护边界日渐模糊。在多数据中心建设过程中，如何同步地部署安全防护，安全策略将成为另一大难题。

参考文献：

[1]张届新，吴志明.基于 VxLAN 组网的云数据中心互联方案[J].电信科学，2016.

[2]曾珊，陈刚，齐法制.高性能云数据中心弹性网络研究[J].计算机工程与应用，2018.

[3]黄伟，赵峰，陈刚，等.基于 VxLAN 的医院多网融合架构研究与应用[J].医学信息学杂志，2019.

[4]李民，曹阳，郭益锋.基于 EVPN 技术的医院网络设计与改造[J].中国数字医学，2018.

浅析互联网医院的发展现状及前景

◆余梦飞

（安徽医科大学第一附属医院　安徽　230000）

摘要：近年来，医疗服务领域新形态不断涌现，互联网医院作为其中突出的一种，在远程诊疗、线上问诊等方面展现出巨大的发展潜力。本文结合互联网医院目前的发展现状，梳理分析互联网医院的发展瓶颈及其优势特点，并提出对于互联网医院未来发展思路的相关思考。

关键词：互联网医院；发展现状；制约因素；优势特点；发展思路

1　引言

“互联网+医疗”是以互联网为主体的信息技术与传统医疗行业深度融合的行业新形态，是我国医疗卫生事业发展的重要趋势[1]。目前“互联网医院”尚无明确的定义,行业内部认为互联网医院是医疗机构直接向患者提供远程医疗服务,即运用信息化技术将医疗资源从医院内部延伸到互联网端,开展在线医疗服务及健康服务的互联网医疗平台[2]。互联网医院，带有咨询、随访、慢病管理等功能，以实体医院作为强有力的依托，通过图文、视频的方式，实现在线问诊、智能问药等，并可选择药品快递到家，互联网医院使民众足不出户就可享受到三甲医院的优质医疗资源,方便快捷、优质高效成为它的魅力所在。

2　互联网医院的发展

互联网医院是“互联网+医疗”终极必然产物。中国互联网络信息中心报告，截至 2016 年底，中国互联网拥有 1.95 亿的医疗用户，占网民总人数的 26.6%；用户使用率最高的是医疗信息查询与网上预约挂号，分别达到 10.8%和 10.4%[3]。

2018 年，国务院办公厅印发《关于促进“互联网+医疗健康”发展的意见》，提出允许医疗机构开展部分常见病、慢性病复诊等互联网医疗服务，为“互联网+医疗健康”明确了发展方向。新冠肺炎期间，国家卫生健康委员会印发通知，要求各地医疗机构充分发挥“互联网+医疗”的独特优势，规范互联网诊疗咨询服务，拓展线上医疗服务空间，引导患者有序就医，缓解疫情传播，各大医院积极响应，迅速开通互联网医院线上门诊，部分医院已实现常态化为发热患者、复诊患者提供门诊诊疗、药品配送、用药及护理咨询等相关服务。微信官方发布数据显示：近年来，我国有上千家医院支持微信挂号，其中有

近百家医院上线微信进行全流程就诊，服务患者超过 300 万、节省超过 600 万小时的患者就医时间[4]。

3　互联网医院的优势

3.1 患者就医体验显著改善

对于没有时间或不方便到院就诊的患者来说，线上就诊消除了地域及时间限制，患者可以随时通过图文咨询或远程视频的方式进行线上问诊，并且互联网医院可提供药品“一站式”配送到家等特色服务，节约了患者大量就医时间和就医成本，在实现服务更多患者的同时，也极大改善了患者的就医体验。

3.2 优质医疗资源明显下沉

很多医疗单位信息化发展水平相对较低，信息孤岛现象突出，医患沟通时间短、患者离院后无法获得医疗机构持续良好的健康追踪和关注[5]，互联网医院的出现，打破了以往医院与患者、医生与患者之间的空间距离，降低了偏远地区及医疗技术水平较不发达地区患者就医难度，又以常见病、多发病、慢性病等为诊治重点，一定程度上缓解了当前“看病难、看病贵”的社会压力，使民众足不出户就可享受到高质量、更便捷的优质医疗资源，有效推动了优质医疗卫生资源的科学配置和科学下沉。

3.3 医院智能化管理水平显著提升

互联网医院的线上问诊数据，如病理数据、检查检验数据、处方数据、药品数据等可在医院内部智能系统清晰可见，相关行政部门可以依托就诊平台抓取到的数据，对相关的医疗数据进行分类分析，为医院加强医疗监管、强化公共卫生服务等提供大数据支撑，实现医院管理的可视化、智能化，提升医院智能化管理水平。

4　互联网医院发展的制约因素

4.1 就诊对象具有局限性

目前互联网医院平台只能实现自费患者的缴费及结算，大多数地方医保目前并未实现互联网支付，这就意味着患者在互联网医院就诊过程中产生的医疗费用无法直接进行医保报销，仍需患者到实体医院进行医保相关的结算。此外，互联网医院作为一个新兴事物，在发展过程中受到传统观念的束缚，一些年龄较大、文化基础较弱的患者对于互联网医院的认知度相对较弱，这些因素就直接影响到民众接受、使用“互联网医院”的范围和程度。

4.2 就诊科室选择性较小

目前，互联网医院开诊科室主要以小病和慢病等普通疾病问诊为主，如内分泌科、皮肤性病科、用药咨询、护理咨询、患者复诊等，对于病情复杂严重、需要做 CT 等相关医学检查确定病因的初诊患者来说，互联网医院目前还不能完全替代实体医院，无法满足病情复杂患者的就医需求，导致患者在就诊科室选择方面存在一定的局限性。

4.3 就诊信息存在安全风险

互联网医院依托互联网技术开展，人们在享受互联网技术带来便捷的同时，信息安全也成为一个不可避免的重要话题，医院信息安全保障显得尤为重要，医院就诊信息不仅包含线上就诊过程中出现的患者个人信息，还包含了医院方面相关的医疗数据，只有筑牢医院网络系统安全屏障，才能确保病人隐私、医疗数据等不被泄露。

4.4 政策法规体系不完善

互联网医院虽然目前发展势头迅猛，但在我国乃至世界范围内仍处于初步探索阶段，相关法律法规、管理政策已远远滞后于现实发展需要，法律体系方面存在较多漏洞，如线上问诊过程中出现的医疗纠纷该如何定责等问题并没有明确的相关界定标准，逐步建立健全对互联网医院这一新生形态的监管体系显得尤为重要。

5　互联网医院未来发展的思考

5.1 共建共享信息平台，切实提供良好服务

近年我国不断加强医院现代化、信息化建设，大部分三级医院完成了信息管理系统（MIS）建设，基层医院信息化建设工作也取得初步成效[6]，但各区域内不同医院之间仍然存在单独建设信息系统等问题，导致信息孤岛，因此，要依托协同公共卫生信息系统、基层医疗卫生管理信息系统、医疗健康公共服务卫生计生资源体系[7]，深入推进各级医疗机构之间信息的互联互通，实现患者电子健康档案、电子病历在不同医疗机构之间实现共享；切实完善医保政策，探索推广互联网医院享有公立医院同等的医保报销政策；试点推广互联网医院在对居民就诊中的导诊作用，推动实现分级诊疗；患者就诊持实名制就诊卡，做好实现互联网医院与实体医院信息交互与业务流程管理。

5.2 全面优化诊疗流程，提升患者就医体验

目前互联网医院运营主要覆盖诊前服务、诊断服务、开方服务、药品服务等几个环节，针对线上就医的患者，必须要保证网络问诊的操作流程清晰明了，这就要求医院信息部门从使用者角度出发，充分考虑老年人和教育程度较低群体的实际应用能力薄弱等因素，不断优化设计网络问诊页面，积极开发简便快捷的医疗就诊 APP，让线上就医流程操作简便又能达到良好的就医效果，确保方便患者的同时又能方便医生。

5.3 加强法律法规建设，提供坚实法治保障

政府部门应加强对互联网医院建设的重视，从保障医患双方利益的角度出发，以互联网医院的实际建设情况为参考，出台相关法律法规，进一步规范互联网医疗市场，尽快制定行业标准，规定医疗信息企业的准入标准、业务范畴、服务模式、权责界定等[8]，确保建设过程中的任何问题都有法可依，保障医生和患者的合法利益不受侵害，从而助力互联网医院持续健康发展。

5.4 确保医护人员资质，提高医疗服务质量

互联网医院的重要特点是对于医疗资源的优化配置和应用，为患者、医护人员提供更加便利的医疗服务管理，因此医院需要加强医疗应用管理水平。一方面需建立严格的筛选标准和考评体系，要求提供医疗服务的医师必须出具相关执业资格证明等，平时还应开展实践培训等活动不断提升医护人员的专业素质和业务能力，确保互联网诊间医护人员的医疗水平，此外，提升医护人员对互联网医院的了解程度也是一项不可或缺的机制，确保诊间医护人员熟练应用医院内部的各个智能系统，提高医疗服务质量和效率。

5.5 加强医院信息系统建设，确保医疗信息安全

互联网医院的线上就诊过程基本上是公开透明的，要想确保相关医疗服务数据的隐蔽性和保密性，就必须以行政部门管控为主，制定医疗服务质量控制标准，为其提供安全的网络技术支持[9]。实体医院也应根据自身实际情况进行适当的资金投入和人力资本投入，引进一些计算机或信息网络建设方面的专业技术人员，积极探索新的网络安全防护技术，加强数据运营管理，依据数据的重要性，对不同数据进行分级安全保障管理；技术上对患者的医疗信息进行加密，数据授权；对工作人员进行安全培训，严格管理，避免出现利用职务便利或操作不当造成信息泄露的情况[10]，建设规范安全的健康医疗数据库，确保患者的就医安全和个人隐私安全。

随着我国经济的不断发展，民众对于医疗服务的需求日益增长，互联网医院虽然目前还是新生事物，但它作为实体医院的补充，极大地提升了医疗服务效率，缓解了看病排队、缴费排队、拿药排队等问题，节约了患者和医护人员双方的时间。我们也应清醒认识到，在技术不断发展的未来，互联网医院还有很大的提升空间，还需要在探索中不断完善，利用互联网医院为病人提供优质便捷的诊疗服务，必将成为今后医疗行业发展的必然趋势。

参考文献：

[1]陈晋阳.“互联网+”视角下健康医疗大数据研究［J］.南京医科大学学报（社会科学版），2017，17（4）：269-272

[2]邱晨，唐铭坚，吴伟晴，等.大型医院深入开展远程医疗服务探索[J].中华医院管理杂志，2016，20（2）：47-49.

[3]夏云红.探讨医院预算的细化与执行[J].今日财富（中国知识产权），2017（12）：129-130.

[4]李颖，孙长学.“互联网+医疗”的创新发展[J].宏观经济管理，2016（3）：33-35.

[5]王叶华，杨丽黎，林辉，等.互联网+在三级医院双向转诊中的应用[J].中华医院管理杂志，2016，32（5）：396-398.

[6]刘宁，陈敏.我国互联网医疗服务模式与应用现状分析[J].中国卫生信息管理杂志，2016（5）：455-460.

[7]李华才.促进“互联网+医疗健康”发展的行动指南[J].中国数字医学，2018，13（6）：1.
[8]晏茜勤.我国互联网医疗运作模式比较研究[J].齐齐哈尔大学学报（哲学社会科学版），2015（10）：56-58.
[9]张振，周毅，杜守洪，等.医疗大数据及其面临的机遇与挑战[J].医学信息学杂志，2014，36（6）：2-8.
[10]李璐，谢颖夫，胡广阔.“互联网+医疗”中信息安全的探讨[J].价值工程，2017，36（9）：49-50.

医院网络终端安全准入系统初探

◆胡少峰　谢新鹏　文海荣

（南方医科大学南方医院增城分院　广东　511300）

摘要：在国家要求全面加强信息安全保障体系建设及落实信息安全等级保护的大背景下，网络安全日渐成为医院信息化建设的重要一环，医院网络接入层作为信息安全防护体系的前沿阵地更应受到重视。本文通过结合医院实际网络情况对网络准入系统的认证模式选型、部署方式、准入效果等进行探究，简述网络终端准入系统在南方医科大学南方医院增城分院（下文简称“本院”）的初步实践，对实施过程中遇到的问题进行讨论与经验总结。

关键词：医院网络安全；准入系统；Mac 认证

1　前言

网络终端安全准入，是通过对终端接入网络实施安全管控的防御技术，建立起终端从登记－准入－监控－下线的全周期防控流程。为防止潜在威胁入侵网络，对医院内网的接入层端口实施安全准入，是保证医院网络安全运行的前提。

随着信息化建设的快速发展和互联网的普及应用，网络安全威胁逐渐升级，医疗机构作为治病救人、保障民生的特殊行业，历来都是网络攻击的首选目标之一。本院于 2018 年底开业，开业初期医院内网的接入层安全防护尚未完善，因为开放式的网络架构，大量的网络端口暴露在院内建筑的各个角落，脆弱的用户终端一旦轻易地接入网络，就等于给潜在的安全威胁敞开了大门，如何加强网络安全的前端防护，保障医院内部网络及数据的安全可靠[1]，是院领导及科室领导关注的问题。

2　准入管理前的内网状况

本院作为新建医院，1 期建设完工并投入使用的主体建筑物主要包括：门（急）诊楼、住院楼、医技楼、传染病楼，各主体建筑内网由中心机房核心交换机直通万兆双路光纤至各楼层光纤配线架，配备千兆交换机约 170 台，经堆叠后汇总可管理的交换机为 46 台。院内内网接入设备种类多、各类设备数量约 1400 台，主要涉及诊室内网 PC、叫号屏、诊间屏、分诊台报到机及自助打印机、药房自动配发药设备、各类专用医疗设备及智能化设备哑终端等。由于医院人员流动性较大，对于非本院工作人员擅自使用设备接入内网的情况于开业前期时有发生，网络安全隐患较突出；没有安全措施且遍布全院的接入点，当网络出现故障时定位故障难度较大，也曾出现过第三方公司驻院期间私建局域网后接入内网引发内网 dhcp 冲突的情况。

3　准入模式的选型

该准入系统基于硬件平台实现，采用 NAC（Network Admission Control）是一种“端到端”的安全结构，包括 Portal 认证、透明网关、策略路由与 802.1X 认证等。

（1）Portal 模式，基于 B/S 模型完成客户端和服务器的交互，需在接入层对终端通过 VLAN 实现访问网络权限的控制，接入的用户强制跳转至特定网页进行认证，通过 Web 页面验证准入。

（2）透明网关模式，需将准入设备串联在内网核心位置，基于包过滤技术对网络中数据进行处理，该模式下终端可通过安装客户端准入，也可用 Web 完成准入。

（3）策略路由模式，同样基于包过滤技术，需在核心交换机上将流量镜像配置至准入设备进行处理，符合条件的流量则正常转发，对不符合条件的流量操作丢弃或重定向，引导用户通过 Web 准入页面完成注册登录后接入内网。

（4）802.1X 模式，基于 Client/Server 的访问控制和认证协议 802.1X，可以通过安装客户端后登录授权的账号密码准入，也可将交换机端口学习到的终端 Mac 地址管控准入。

在准入系统的选型过程中，我们主要考虑系统的部署方式对业务网络的影响、各类终端的管控适用性、准入模式的可靠性及可操作性。在透明网关模式下，需串联在网络核心位置，鉴于系统上线期间需中断业务网络，且串联在网络中存在运维风险，一旦设备宕机将造成全网故障，故不考虑此模式；在 802.1X 模式、策略路由和 Portal 准入模式下，将旁路部署在核心网络中如图 1 所示，系统调试及上线对业务皆无影响，但因兼顾多类终端（部分终端无法安装客户端或使用 Web 准入）适用性，且在准入模式不可混合开启情况下，最终选定 802.1X 协议下 Mac 认证模式作为统一准入模式，该模式下连接到同一端口的每个设备都需要单独进行认证。

图 1 准入设备部署网络架构图

4　802.1X—Mac 模式下系统架构及功能

典型 802.1X 系统为的 Client/Server 结构，包括：客户端、设备端和认证服务器等实体[2]，该准入系统基于硬件平台实现，部署 802.1X—Mac 模式主要涉及 radius 认证服务器端和接入交换机端的配置，本院接入层皆部署支持 802.1X 的三层可管理交换机，准入设备与交换机之间无 NAT 防火墙等一些疑似替换 Mac 的设备。准入系统提供的 Web、telnet 等后台管理界面，准入系统主要应用功能如下：

（1）网络设备管理：认证管理后台添加相应交换机管理 IP，并与交换机同步开启 snmp 网管协议，服务器通过 snmp“读”“写”操作对交换机的配置、参数、端口状态等进行管控，并有设备实时可视化管理界面。