医院网络架构仿真研究*

徐 皓 李超凡 张梦娜 任 鹏 张 然

（徐州医科大学医学信息与工程学院 徐州 221000）

〔摘要〕 从逻辑网络拓扑、实施方案等方面阐述医院网络架构仿真设计，介绍相关技术，经仿真实验验证该架构可实现流量负载与冗余备份，路由区域划分合理，提升医院网络资源利用率。

〔关键词〕 医院网络架构；EVE－NG；虚拟路由冗余；多生成树协议；可扩展性

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2021.01.013

Study on the Simulation of Hospital Network Architecture *XU Hao, LI Chaofan, ZHANG Mengna, REN Peng, ZHANG Ran, College of Medical Information and Engineering, Xuzhou Medical University, Xuzhou 221000, China*

〔**Abstract**〕 The paper elaborates the simulation design of hospital network architecture from the aspects of logical network topology, implementation scheme, etc., introduces related technologies. The simulation experiment verifies that this architecture can realize traffic load and redundant backup, reasonably divide routing area, and improve the utilization rate of hospital network resources.

〔**Keywords**〕 hospital network architecture; EVE－NG; virtual routing redundancy; Multiple Spanning Tree Protocol (MSTP); scalability

1 引言

根据《健康中国2030规划纲要》，我国正努力推进现代化数字医院与健康医疗大数据应用体系建设，消除医院数据壁垒，建立跨领域、跨部门的医疗数据共享机制，全面提高医疗信息服务质量。医院网络是提高医疗服务效率、建立健康医疗数据平台的基础，高可用性与稳定性是医院网络最基本性能需求，可扩展性是医院信息业务拓展的重要保障[1]。在医院网络平台建设过程中，为兼顾稳健性与可扩展性，通过仿真实验负载均衡、冗余备份、网络资源利用率、服务质量等方面综合分析，设计并搭建逻辑网络拓扑，实现网络平台自动防环与故障恢复，同时融合动态路由协议与基于端口的地址转换技术，提供医院内部信息交互与访问互联网的安全服务。

〔修回日期〕 2020－05－28

〔作者简介〕 徐皓，本科，工程师，发表论文1篇；通讯作者：张然，博士，讲师。

〔基金项目〕 江苏省高等学校自然科学研究项目“干扰环境下WBAN跨层优化设计研究”（项目编号：19KJB520062）；江苏省大学生创新创业训练计划“医院网络突发故障事前深度分析与安全运维平台MNSSfire的设计与构建”（项目编号：201810313089H）；徐州医科大学优秀人才科研启动基金项目“基于压缩感知的人体生理信号分析”（项目编号：D2019032）。

2 相关技术

2.1 多生成树协议

多生成树协议（Multiple Spanning Tree Protocol，MSTP）相比生成树协议（Spanning Tree Protocol，STP）或快速生成树协议（Rapid Spanning Tree Protocol，RSTP）具有虚拟局域网（Virtual Local Area

Network，VLAN）认知、负载均衡、端口状态快速切换、快速收敛以及向下兼容 STP/RSTP 协议等显著优势[2]。其主要由 MST 域、公共生成树、公共与内部生成树组成。MST 域（MST Region）将二层网络划为多个 MST 域，每个域内单独计算生成多个实例 MSTI（MST Instance），通过 VLAN 映射表实现多 VLAN 与单 MSTI 映射，实例 ID = 0 的内部生成树（Internal Spanning Tree，IST）通过 RSTP 计算生成公共与内部生成树[2]。公共生成树（Common Spanning Tree，CST）由二层交换网络内多个 MST 域中通过 STP 或 RSTP 计算最优路径产生的区域型生成树，用于将各 MST 域连接为统一整体。公共与内部生成树（Common Internal Spanning Tree，CIST）是由每个 MST 域的 IST 与域间的 CST 组成的根生成树，CIST 中的根设备为整个二层网络的根桥[3]，自顶向下与各 MST 域的 IST 域根组成多个无环生成树。

2.2 虚拟路由器冗余协议

虚拟路由器冗余协议（Virtual Router Redundancy Protocol，VRRP）是一种将一组或多组物理路由器抽象为一台主设备与多个备份设备组成的逻辑路由器的容错协议。利用虚拟路由标识符（Virtual Route IDentifier，VRID）标记同组设备进行角色协商，完成后通过主设备的 VRRP 报文通告全组。一组 VRRP 设备使用统一虚拟 IP 与 MAC 地址作为用户默认网关，监控上层端口状态，同时提供底层设备逻辑接入。医院内网出现设备单点故障后，核心网络仍然提供高可用性的缺省链路，避免医院信息系统网络服务中断的问题[4]。

3 医院网络架构仿真

3.1 概述

使用 EVE－NG 虚拟仿真平台搭建医院内网拓扑，核心交换机使用华为 S12700 系列敏捷交换机镜像，汇聚层使用华为 5700 系列交换机镜像，出口防火墙使用思科 FirePower9000 系列进行融合组网，通过 SecureCRT 连接虚拟节点进行路由配置。

3.2 逻辑网络拓扑

以徐州市某三甲医院为例，按照分权分域原则，将整个医院门诊大楼、住院部、行政楼、医学技术楼、后勤保障楼划为内网接入区域，数据中心与网管平台划为内网应用区。通过调研医院日常开展医疗业务流量开销，根据网络稳定性、利用率、延时、冗余等不同需求，针对不同区域进行相应设计：在内部接入区，依据各建筑相应职能划分多个 VLAN，实现广播隔离与多出口冗余；在核心交换区，针对汇聚层与核心层交换机，采用 VRRP 与 MSTP 实现核心网关冗余与流量负载均衡，达到主备核心交换机相互备份且共同承载数据转发压力的效果；专网出口区域通过开放式最短路径优先协议（Open Shortest Path First，OSPF）合理划分区域，汇聚路由地址信息，使用端口多路复用技术，减少通信开销，实现数据共享与接口预留[5]。医院内网总体逻辑架构，见图 1。

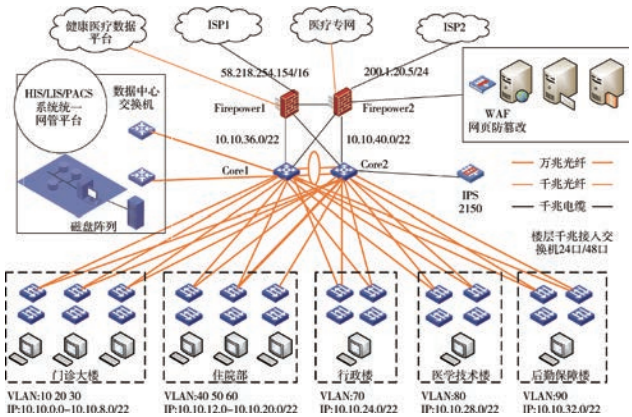

图 1 医院内网总体逻辑架构

3.3 实施方案

3.3.1 概述 实施方案主要分为两部分：第 1 部分采用 VRRP 与 MSTP 融合技术，将两台核心层物理交换机虚拟为 1 台逻辑设备，通过相应业务 VLAN 进行主备链路切换与流量负载均衡；第 2 部分使用 OSPF，划分路由区域，通过端口多路复用技术减少外网通信开销，实现医院内网路由汇聚与互联网通信。

3.3.2 第1部分 将门诊大楼、住院部等依据业务需要与地理位置划分相应VLAN。核心层与汇聚层交换机通过MSTP将VLAN10－60捆绑实例Instance1，设置Core1交换机为Instance1的根交换机，Core2交换机为备份根交换机，实现门诊大楼与住院部业务流量转发主链路为Core1设备，备份链路为Core2设备。同时VLAN70－90捆绑实例Instance2，主链路转发路径与实例Instance1相反，生成树中根交换机为Core2设备，实现整个核心网络的负载均衡[6]与链路双向冗余备份。通过VRRP技术将VLAN划分成9个VRRP组，建立VRRP组与业务VLAN一对一映射。将行政楼、医学技术楼、后勤楼添加至Core2为主、Core1为辅的VRRP虚拟备份组[4]，门诊大楼与住院部设置与上述相反。核心层双设备全部开启端口状态追踪，针对上行链路端口实时监听，实现链路故障自动切换的容错机制，达到不间断通信的目的。

3.3.3 第2部分 在专网出口防火墙与核心层交换机之间运行OSPF，进程号设置为110，将两台防火墙Firepower之间设置为骨干区域Area0，将Firepower防火墙与两台核心交换机之间分别设置为区域Area1与Area2，将区域Area1与Area2分别汇聚相应两台核心交换机与汇聚层交换机路由信息，完成医院内网各区域的互联互通。路由汇总后，在两台Firepower防火墙开启基于端口复用的地址转换，将医院内网汇总为统一网段，通过端口复用完成内网到公网IP地址的多对一映射，保证医院内外网通信与数据传输[6]。同时在Firepower1防火墙预留健康医疗数据平台专网互联端口，保证可扩展性。

4 验证与分析

4.1 第1阶段

整个设计方案的效果验证与数据分析主要分为3个阶段。第1阶段验证与分析包括MST域中，实例Instance1通过STP或RSTP计算生成以Core1设备为主根交换机，Core2设备为主链路失效后备份根交换机的核心流量传输路径。实例Instance2则生成相对的以Core2设备为主路径，Core1为备份转发路径的生成树。门诊大楼、住院部的汇聚层交换机去往Core1设备链路处于转发状态，而去往Core2设备链路处于阻塞状态，STP生成树端口状态，代码如下：

<Core1>display stp instance 1 brief

MSTID	Port	Role	STP State	Protection
1	GigabitEthernet0/0/1	DESI	FORWARDING	NONE
1	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
1	GigabitEthernet0/0/3	DESI	FORWARDING	NONE
1	GigabitEthernet0/0/4	DESI	FORWARDING	NONE
1	GigabitEthernet0/0/7	ROOT	FORWARDING	NONE

<Core1>display stp instance 2 brief

MSTID	Port	Role	STP State	Protection
2	GigabitEthernet0/0/1	DESI	FORWARDING	NONE
2	GigabitEthernet0/0/2	DESI	FORWARDING	NONE
2	GigabitEthernet0/0/3	DESI	FORWARDING	NONE
2	GigabitEthernet0/0/4	ROOT	FORWARDING	NONE
2	GigabitEthernet0/0/7	DESI	FORWARDING	NONE

4.2 第2阶段

主要包括VRRP备份组中Master和Backup设备进行主备协商，协商完成产生虚拟网关设备，生成虚拟IP与MAC地址。当主设备链路出现故障后，备份设备瞬时切换角色，进行数据流量转发。验证方案采用双向数据联通性测试，首先测试Core1主设备故障时，门诊大楼客户端链路切换速率，其次测试Core2主设备链路故障时，后勤楼客户端链路切换速率，测试结果如下。传输100个网际控制报文协议（Internet Control Messages Protocol，ICMP）报文平均丢包率为2%，平均传输时延为58.5ms，实现两台核心交换机相互备份，同时VRRP主设备故障时备份设备秒级链路切换，保证医院网络服务不间断。

```
< A1 - 1 > ping - c 100 10. 10. 0. 1
PING 10. 10. 0. 1: 56 data bytes, press CTRL c to break
Reply from 10. 10. 0. 1: bytes = 56 Sequence = 1 ttl = 255 time = 90ms
Reply from 10. 10. 0. 1: bytes = 56 Sequence = 2 ttl = 255 time = 60ms
Reply from 10. 10. 0. 1: bytes = 56 Sequence = 3 ttl = 255 time = 70ms……
Reply from 10. 10. 0. 1: bytes = 56 Sequence = 99 ttl = 255 time = 80ms
Reply from 10. 10. 0. 1: bytes = 56 Sequence = 100 ttl = 255 time = 50ms
- - - 10. 10. 0. 1 ping statistics - - -
100 packet (s) transmitted
98 packet (s) received
2. 00 packet loss
round - trip min/avg/max = 30/60/100 ms
```

4.3 第 3 阶段

该阶段效果验证与报文分析包括 OSPF 的路由汇聚与端口多路复用的公网映射过程，出口防火墙与核心层交换机划分 OSPF 区域[5]，进行区域互联与路由汇聚，将核心层设备中的多个业务 VLAN 管理网段汇聚为统一网段：10. 10. 0. 0/22，在防火墙进行端口多路复用设置，将内网统一网段进行公网映射，转换为公网“IP：端口号”的形式。验证方案采用内网接入区域客户端访问测试外网。分析报文源地址与目的地址的映射，门诊大楼客户端以 IP 地址 10. 10. 0. 100 访问外网时，形成多对一以套接字形式的［58. 218. 254. 154：端口号］进行互联网访问，通过套接字实现公网地址复用，减少通信开销。整个设计方案在保证内网高度稳定的前提下实现医院内网与外网不间断通信。测试结果如下：

```
Firepower#debug ip nat
* Mar 1 00: 56: 20. 343: NAT *: s = 58. 218. 254. 155, d = 58. 218. 254. 154 - > 10. 10. 40. 2 [17]
* Mar 1 00: 56: 20. 367: NAT *: ICMP id = 3 - > 7
* Mar 1 00: 56: 20. 367: NAT *: s = 10. 10. 40. 2 - > 58. 218. 254. 154, d = 58. 218. 254. 155 [18]
* Mar 1 00: 56: 20. 387: NAT *: ICMP id = 7 - > 3
* Mar 1 00: 56: 20. 411: NAT *: s = 58. 218. 254. 155, d = 58. 218. 254. 154 - > 10. 10. 40. 2 [18]
* Mar 1 00: 56: 20. 411: NAT *: ICMP id = 3 - > 7
* Mar 1 00: 56: 20. 431: NAT *: s = 10. 10. 40. 2 - > 58. 218. 254. 154, d = 58. 218. 254. 155 [19]
```

Pro	Inside global	Inside local	Outside local	Outside golbal
icmp	58. 218. 254. 154: 2	10. 10. 36. 3: 2	58. 218. 254. 155: 2	58. 218. 254. 155: 2
icmp	58. 218. 254. 154: 7	10. 10. 40. 2: 3	58. 218. 254. 155: 3	58. 218. 254. 155: 7
icmp	58. 218. 254. 154: 3	10. 10. 44. 4: 3	58. 218. 254. 155: 3	58. 218. 254. 155: 3

5 结语

医院内网承担着所有信息化业务的数据传输，医院内网仿真实验表明基于冗余备份与负载均衡的网络架构，能够实现医院网络数据传输的高可用性与稳定性，满足医院对于网络可靠性的性能需求。同时动态路由协议与端口复用的地址转换技术相融合，提升网络资源利用率，在保障网络稳定性的前提下确保医院信息系统间高效的信息交互。

参考文献

1 高翔，黄文康，詹孙茹. 民族医药移动信息平台设计与实现［J］. 医学信息学杂志，2019，40（7）：35 - 39.

2 贺吉群，成鹏飞，肖映平，等. 网络信息技术在优化手术病人转运过程中的应用［J］. 医学信息学杂志，2016，37（10）：48 - 51.

3 王修来，张伟娜. 数字化医院建设中移动临床信息系统的开发与应用［J］. 医学信息学杂志，2011，32（9）：16 - 18.

4 陈延东. MSTP + VRRP 技术在校园网双核心中的应用［J］. 产业与科技论坛，2016，15（4）：52 - 53.

5 陶骏，严志兵，颜云生，等. 基于 OSPF 和 NAT 的企业网络构建［J］. 通化师范学院学报，2018，39（10）：51 - 54.

6 刘开森，李天赐，李胜辉，等. 基于 OSPF 和 NAT 企业网可靠性和安全性仿真实验设计［J］. 网络安全技术与应用，2018（6）：31 - 33.