 DOI: https://doi.org/10.12345/bdai.v6i2.24595

Design of intelligent medical network based on Pnetlab

Yaqin Shang Xiaolin Zhang* Yang Cao

School of Computer and Software Engineering, University of Science and Technology Liaoning, Anshan, Liaoning, 114051, China

Abstract

Based on the background of intelligent medical treatment, this paper uses Pnetlab to design and build the network architecture of A large general hospital. This design uses Enhanced Internal Gateway Routing Protocol (EIGRP), Port Security, DHCP Snooping, IP Source Guard (IP SG), dynamic ARP Examine (DAI), multiple spanning Tree Protocol (MSTP), BGP routing, route readvertisement, network address translation (NAT), routing policy and other related technologies to ensure data security, network stability, communication efficiency, and improve the reliability of medical networks. This design scheme aims to provide useful reference for network enthusiasts or technicians in related fields.

Keywords

Pnetlab; smart medical; network architecture; communication

基于 Pnetlab 的智慧医疗网络设计

商亚琴 张孝临* 曹杨

辽宁科技大学计算机与软件工程学院，中国·辽宁 鞍山 114051

摘 要

本文以智慧医疗为背景，利用Pnetlab设计搭建了大型综合医院A医院的网络架构，本设计使用了增强型内部网关路由协议（EIGRP）、端口安全（Port Security）、DHCP Snooping、IP Source Guard（IP SG）、动态ARP检查（DAI）、多生成树协议（MSTP）、BGP路由、路由重发布、网络地址转换（NAT）、路由策略等相关技术，以确保数据安全、网络稳定、通信高效，提高医疗网络的可靠性。此设计方案旨在为网络爱好者或相关领域的技术人员提供有益参考。

关键词

Pnetlab；智慧医疗；网络架构；通信

1 引言

A 医院概况为：除总院外，医院还设有两个分院，这里我们分别命名为北京总院、天津分院、河北分院，该医院提供全方位的医疗服务，涵盖内科、外科、放射科、急诊科、实验室等各个科室。为提升医疗服务质量和效率，A 医院计划建设一套先进的智慧医疗网络系统，以满足现代化医疗需求，确保数据安全、网络稳定、通信高效。

通过 Pnetlab 工具构建 A 医院智慧医疗网络架构，为医院各科室（如内科、外科、急诊科等）提供高效的数据传输和资源调度支持，搭建覆盖总院与分院的统一智慧医疗网络 [2]，保障医疗数据的互联互通，实现远程会诊、资源共享和业务协同，提升跨区域医疗服务能力。引入先进的网络安全技术（如端口安全、DAI、访问控制等），以应对医疗数据传输中的信息泄露和网络攻击风险，保障患者隐私以及增强医疗业务稳定性。也希望通过智慧医疗网络的设计能够为行业发展提供参考，推动智慧医疗技术的落地与推广。

2 Pnetlab 简介

PNETLab（全称为分组网络仿真器工具实验室）作为一款专业网络仿真平台，主要服务于网络技术的教学研究、方案验证及系统测试等应用场景。该平台通过构建虚拟化网络环境，使教育工作者与工程技术人员能够在不依赖实体设备的前提下，开展计算机网络系统的模拟操作，从而深化理论认知并提升实践能力。其系统架构具有跨平台特性，支持在 Windows、Linux 和 macOS 等主流操作系统上部署运行 [1]。平台内置的网络实验资源库涵盖网络基础设施构建、安全策略实施等典型应用场景，支持即装即用和定制化开发需求。其图形化操作界面集成网络拓扑构建、设备参数配置及运行监控等功能模块，并内置 Wireshark 等数据包分析工具，便于开展网络流量监测与协议解析工作。在设备兼容性方面，系统完整模拟路由器、交换机、防火墙等网络设备的运行环境，支持虚拟设备的互联互通与集中管控。在协议支持层面，平台完整覆盖 IPv4/IPv6 双栈协议、路由协议（OSPF、RIP、BGP）、交换技术（VLAN、MPLS、VXLAN）、高

可用机制(VRRP、集群、双机热备)以及软件定义网络(SDN)等协议体系，有效保障了实验设计的完整性和方案实施的可扩展性。

3 技术支持

本项目运用到的技术有：点对点协议（PPP）、虚拟局域网（VLAN）、端口安全（Port Security）、开放式最短路径优先协议（OSPF）、访问控制列表（ACL）、增强型内部网关路由协议（EIGRP）、动态主机控制协议（DHCP）[3]、静态路由与浮动静态路由、DHCP Snooping、IP Source Guard(IP SG)、动态 ARP 检查(DAI)、多生成树协议(MSTP)、端口聚合、网关冗余、BGP 路由、路由重发布、网络地址转换(NAT)、路由策略等技术，下面仅介绍相关的几种技术：

3.1 DHCP Snooping

DHCP Snooping 安全防护机制作为动态主机配置协议（DHCP）的关键加固技术，通过实施数据包监控与过滤策略，有效防范非法 DHCP 服务器仿冒攻击及异常地址分配行为。在智慧医疗网络应用场景中，该机制通过建立可信地址分配体系，确保医生工作站、医学影像设备等关键终端始终获取合法网络配置。具体而言，当医疗设备接入网络时，DHCP Snooping 将严格验证 DHCP 交互流程：在接入层交换机设置信任端口指向中心化 DHCP 服务器，阻断来自非信任端口（如患者访客网络端口）的伪造响应报文。同时，基于动态维护的绑定表信息，可快速定位异常地址分配行为，防止 IP 地址冲突导致的医疗设备断网事故，显著提升医疗业务网络的抗攻击能力和服务连续性。

3.2 IP Source Guard（IP SG）

IP Source Guard（IP SG）是一种基于 DHCP Snooping 绑定表的安全技术，用于验证设备的 IP 地址和 MAC 地址是否匹配，防止 IP 地址欺骗攻击。该技术需要与 DHCP Snooping 绑定表相结合从而才能对接入设备的 IP 地址、MAC 地址和端口信息进行验证。支持绑定表中不存在的非法设备的阻止功能。在智慧医疗网络中，通过 IP Source Guard 防止非法设备伪造合法 IP 地址进行网络攻击，保护关键医疗设备的数据传输安全。

3.3 动态 ARP 检查（DAI）

动态 ARP 检查（Dynamic ARP Inspection，DAI）作为数据链路层安全防护机制，通过与 DHCP Snooping 绑定表联动实现对 ARP 协议报文的深度安全管控。该技术通过校验 ARP 请求与响应报文中的源 IP 地址、目标 IP 地址及 MAC 地址映射关系，有效防范 ARP 缓存投毒（ARP Spoofing）等网络攻击行为。在智慧医疗网络中，启用 DAI 防止 ARP 欺骗攻击，保护医疗设备的网络通信安全，避免关键数据被截获或篡改。能够提供基于 ARP 的二层网络安全防护，防止中间人攻击和流量重定向。

3.4 BGP 路由

边界网关协议（Border Gateway Protocol，BGP）是一种用于不同自治系统（AS）之间路由交换的协议，主要应用于广域网和跨区域网络环境 [4]。BGP 路由能够通过路由策略的灵活配置，优化数据传输路径，提高网络的稳定性和可控性。在智慧医疗网络中，BGP 被用于医院总院与分院、医院与云平台之间的路由传输，通过精确的路由选择和策略过滤，实现医疗数据的高效跨区域传输。

4 智慧医疗网络设计与规划

如下图 1 所示为 A 医院的智慧医疗网络总体架构：

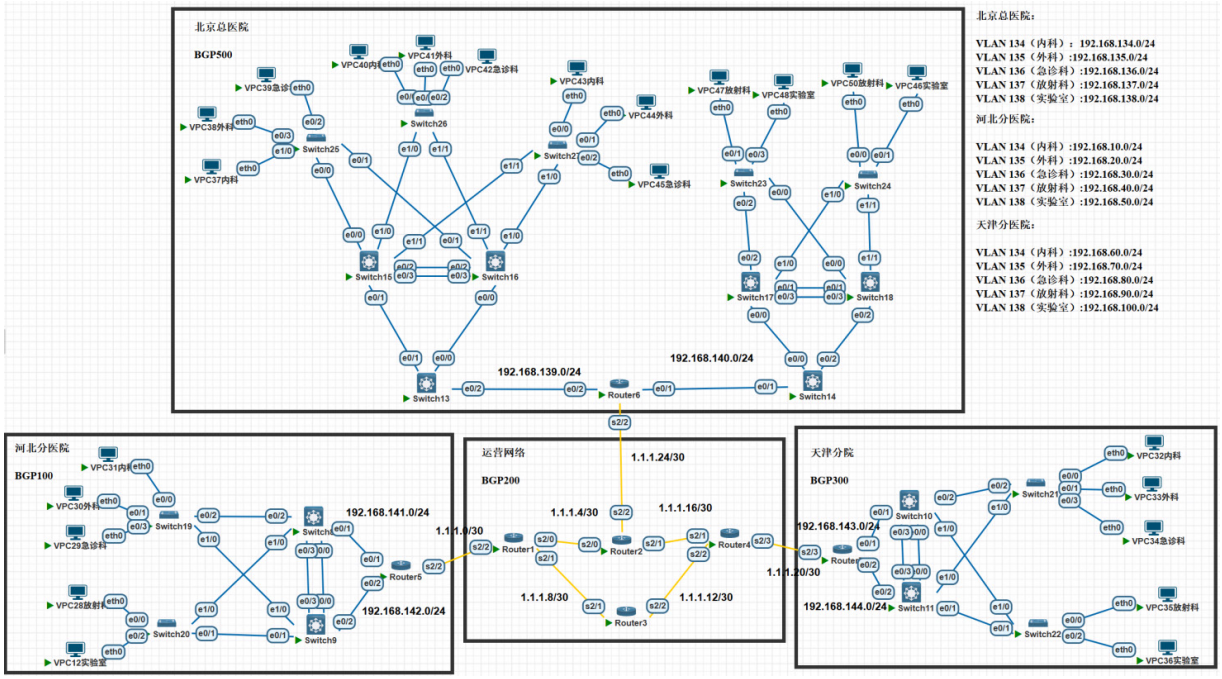

图 1 A 医院智慧医疗网络架构拓扑图

4.1 网络架构——区域划分

A 医院智慧医疗网络根据业务需求划分为三个主要区域：北京总院网络、河北分院网络和天津分院网络。这三个区域各自独立运行，具备完善的网络功能和管理体系，确保区域内部的业务独立性和高效性。同时，各区域通过统一的路由协议实现互联互通，便于医疗数据的高效流转和协作。

作为网络核心区域，北京总院承担全院核心业务的处理和数据中心的集中部署。具备高性能的核心交换设备，用于连接医院内的各科室（如急诊、内科、放射科）和关键业务设备（如影像存储设备、电子病历系统）。使用 VLAN 技术 实现科室与业务的逻辑隔离，例如将患者监护设备、医生工作站和影像设备划分为不同的 VLAN，可提高网络性能与安全性。MSTP（多生成树协议）用于避免二层网络中的环路，提升链路的冗余性和稳定性。端口聚合在核心交换机与汇聚交换机之间提供更高带宽的链路支持，确保医疗影像与实时监护数据的流畅传输。

河北分院负责承载部分医疗服务和与总院的互联互通，部署了区域汇聚交换设备，通过 OSPF 动态路由协议 与总院建立高效的路由连接，实现医疗数据的动态传输。利用静态路由和浮动静态路由，在必要时为医院与总院之间提供稳定的备用路径。分院内部网络同样采用 VLAN 和 DHCP 技术，为终端设备（如医生终端、患者监护仪）提供逻辑隔离和自动 IP 地址分配。

天津分院与河北分院的架构相似，同样作为分布式区域，承担日常医疗数据处理和部分患者服务。通过部署 EIGRP 动态路由协议用于接入层与汇聚层之间的高效路由传输。端口安全（Port Security）在接入层交换机中启用，防止未经授权的设备接入网络。使用 DHCP Snooping 和 IP Source Guard（IP SG）技术，确保终端设备的 IP 地址和 MAC 地址合法性，杜绝非法设备的接入。

各区域间通过 BGP 路由协议 实现高效的跨区域医疗数据传输，同时结合 路由策略 优先保障关键医疗业务的传输路径。部署路由重发布技术实现 OSPF、EIGRP 和 BGP 之间的路由信息共享，确保网络连通性，实现路由优化功能。在广域网互联链路上使用 PPP 协议 提供链路认证和加密，提升数据传输的安全性。

4.2 网络安全——冗余备份：

为了保障 A 医院智慧医疗网络的高可用性和关键业务的稳定运行，在核心网络和区域关键节点部署了冗余备份机制：

核心网络冗余：总院和分院配置了两台三层核心交换机，即双核心设计，网关冗余协议实现设备冗余备份。当主核心交换机出现故障无法正常工作时，备用交换机就发挥了它的显著作用，它可以快速接管核心交换机的业务，确保网络通信的连续性，保障作业正常工作。将端口聚合技术部署于核心交换机与汇聚交换机之间起到链路连接作用，聚合多条物理链路能够提升带宽和冗余能力，满足大流量医疗数据（如影像数据传输）的需求。

路由冗余：配置浮动静态路由作为动态路由协议（如 OSPF 或 EIGRP）的备份路径，确保在主路径发生故障时，网络能够快速切换到备用路径，提升路由稳定性。BGP 路由协议支持分院和总院之间的跨区域路由冗余部署，保障远程医疗、跨区域协作数据的无中断传输。

关键节点冗余：在重要接入层设备和医疗设备的连接中，通过端口安全、DHCP Snooping、动态 ARP 检查（DAI）等技术防止非法接入和网络攻击，提升安全性与设备可靠性。

4.3 网络连通性——区域联通

为了实现总院与分院网络以及内部子区域之间的高效互联，智慧医疗网络采用以下设计：

路由协议与策略优化：总院与分院之间采用 OSPF 或 BGP 动态路由协议，保障医疗数据传输的高效性与稳定性。路由重发布技术用于整合 OSPF 与 BGP 路由协议，实现不同网络区域的无缝互联，支持医疗业务的灵活扩展。

VLAN 和多区域通信：在各区域内部，采用 VLAN 技术对科室网络进行逻辑隔离，如将急诊、内科和外科划分到不同的 VLAN 中，减少广播域范围，提升网络性能。通过 Trunk 模式配置多 VLAN 间的通信，结合 MSTP（多生成树协议）避免环路，同时实现链路的负载均衡，提升网络稳定性。

IP 地址分配与设备接入：配置 DHCP 服务为终端设备（如医生工作站、监护仪、影像设备）自动分配 IP 地址，同时启用 DHCP Relay 功能支持跨子网设备的接入。结合 IP Source Guard 和动态 ARP 检查，防止非法设备接入与网络攻击。

5 总结

本文以智慧医疗为背景，基于 Pnetlab 平台设计实现了一套完整的医院网络架构方案。通过对 A 医院（包含北京总院、天津分院和河北分院）的网络需求分析，采用分层架构设计思路，运用 VLAN 技术实现网络逻辑分区，部署 EIGRP、OSPF 和 BGP 等路由协议确保区域间的高效通信。通过端口安全、DHCP Snooping、IP Source Guard 和动态 ARP 检查等技术，构建了全方位的安全防护体系；采用双核心设计、链路冗余和浮动静态路由等机制，确保网络的高可用性。本设计方案不仅实现了医院各科室间的高效协同和数据共享，也为医疗数据的安全传输提供了可靠保障，希望本网络设计可为同类医疗机构的网络建设提供有益参考。

参考文献

[1] 姚友军.使用pnetlab搭建网络专业理实一体化教学、实验平台[J].电子质量,2022,(04):64-66+74.

[2] 徐皓,李超凡,张梦娜,任鹏,张然.医院网络架构仿真研究[J].医学信息学杂志,2021,42(01):64-67.

[3] 李超凡,刘琼,李民玺,徐皓,马凯.医院虚拟专用网络研究与仿真设计[J].中国数字医学,2020,15(10):91-93.

[4] 熊建辉,卢宇,郑中华.基于EVE-NG的BGP路由协议研究与仿真[J].实验室研究与探索,2020,39(02):101-107.