基于 VXLAN 的医院多网融合架构研究与应用

黄 伟 赵 峰 陈 刚 周 振 朱华东 朱萍萍 王晓梅

（皖南医学院弋矶山医院 芜湖 241001）

〔摘要〕 以皖南医学院弋矶山医院为例，阐述可扩展虚拟局域网络报文格式、传输模型以及基于可扩展虚拟局域网的多网融合架构设计、应用与成效，指出该架构可降低投入成本，更好地服务于临床工作，使运维简单化，方便患者就诊等。

〔关键词〕 可扩展虚拟局域网络；虚拟化专网；多网融合；无状态网络

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2019.01.007

Study and Application of Hospital Multi Network Convergence Infrastructure Based on VXLAN *HUANG Wei, ZHAO Feng, CHEN Gang, ZHOU Zhen, ZHU Huadong, ZHU Pingping, WANG Xiaomei, Yi La Shan Hospital of Wangnan Medical College, Wuhu 241001, China*

〔**Abstract**〕 Taking Yi La Shan Hospital of Wangnan Medical College as an example, the paper dilates on message format transmission model of Virtual eXtensible Local Area Network (VXLAN), and the infrastructure design, application and effectiveness of multi network convergence based on VXLAN, as well as points out that the infrastructure is able to lower input costs, serve clinical practices better, simplify operation and maintenance and facilitate patients in seeking medical consultation, etc.

〔**Keywords**〕 Virtual eXtensible Local Area Network (VXLAN); virtualization private network; multi network convergence; stateless network

1 引言

随着国家“互联网＋医疗健康”指导意见的出台，医疗信息化水平对创新医疗服务模式，提高医疗服务能力和效率，进一步实现信息惠民、惠医、惠政方面的作用日益重要。医疗信息化水平的提升离不开高可用性的基础网络架构支撑，传统的医疗信息网络架构采用物理隔离内外网的方式在智慧医疗战略推进过程中逐渐显露弊端。本研究旨在运用基于可扩展虚拟局域网络（Virtual eXtensible Local Area Network，VXLAN）的多网融合技术解决传统医院信息网络相互孤立、管理成本高、可扩展性差的问题，为打造信息互联互通的智慧医院提供保障。

2 可扩展虚拟局域网络

2.1 VXLAN 报文格式

VXLAN 是基于 IP 网络、采用 MAC in UDP 封

〔修回日期〕 2018－08－08

〔作者简介〕 黄伟，助理工程师；通讯作者：赵峰，高级统计师。

装形式的 2 层虚拟专用网（Virtual Private Network，VPN）技术。引入 8 字节的 VXLAN 报头，包含 24bit 的 VNI 和一些保留比特。加上 UDP/IP/Ethernet 报文头，比原始的 Ethernet 帧增加 50 字节的开销，其报文格式，见图 1。将原始 2 层帧以及 VXLAN 报头封装在用户数据报文协议（User Datagram Protocol，UDP）中，以此穿越 3 层网络，实现在 3 层网络上传输 2 层数据帧[1]。

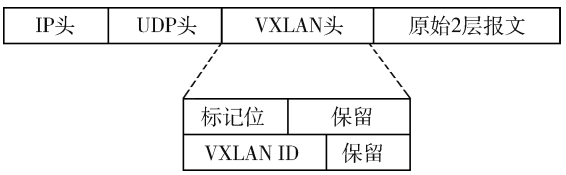

图 1 VXLAN 数据报文格式

2.2 传输模型

VXLAN 是由 NVE、VTEP、VXLAN 隧道、VXLAN 网关几部分组成，其中 VXLAN 网关分为 2 层和 3 层。NVE 为网络虚拟边缘节点，是实现网络虚拟化功能的网络实体。报文经过 NVE 封装转换后 NVE 间可基于 3 层基础网络建立 2 层虚拟化网络。设备和服务器上的虚拟交换机 VSwitch 都可以作为 NVE。VTEP 是 VXLAN 隧道端点，封装在 NVE 中，VTEP 根据 2 层数据包识别 2 层数据报文所对应 VXLAN 的 VIN 号，对数据报文进行封装和解封装。VXLAN 隧道是在不同地理位置之间的 VTEP 或者 VTEP 和 VXLAN 网关之间建立的点对点隧道，用于 VXLAN 数据传输。每个 VTEP 设备都会根据收到的数据包自动维护包含目的 MAC、VIN 号、以及下一跳地址的 VIN 转发表项，VTEP 设备根据此转发表在 VXLAN 隧道中传输数据。VTEP 网关用于不同 VXLAN 之间或者 VLXAN 和原始 VLAN 之间的数据转发。VXLAN 网关所在的 VTEP 设备在收到数据报文后根据 VIN 转发表判断此次转发是 2 层转发还是跨 VIN 的 3 层转发[2]。VXLAN 传输模型，见图 2。在服务器之间进行数据传输时虚拟机首先将数据发送给 VTEP 设备，VTEP 在接收到服务器发送的数据包后根据数据报文的接收端口、VAIN 号等信息识别出该数据报文对应的VLXAN号，然后采用头端复制的方式对原始数据封装后交给承载网络进行转发。如果是同一个 VXLAN 内流量，直接通过 VXLAN 隧道发送给远端 VTEP，再由远端 VTEP 对接收到的数据报文解封装后发送给目的虚拟机。如果是跨 VNI 间的流量，封装数据包首先发给 VXLAN 网关，VLXAN 网关在进行外层封装后根据 VIN 转发表通过组播协议以地址解析协议（Address Resloution Protocol，ARP）泛宏的方式逐级转发给下一跳设备，最终完成跨 VIN 的数据传输。

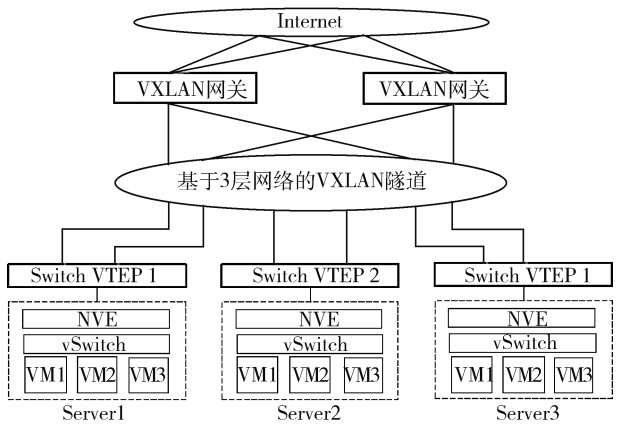

图 2 VXLAN 传输模型

2.3 网络现状

目前采用外网和内网物理隔离的方式，两套网络分别运行在单独的一套物理设备上，无法直接通信，通过在中间部署网闸设备按需控制内网和外网互访。该网络结构下存在以下问题：从核心到汇聚再到接入 3 层设备需要安装两套；要获取内外网资源需采用两台终端或两条链路的方式；隔离区（Demilitarized zone，DMZ）同时连接内外网存在很大安全隐患。此种部署模式造成很大资源浪费，增加管理人员运维的复杂性。医院传统内外网物理隔离网络架构，见图 3。目前采用 OSPF + STP + VRRP 模式部署，汇聚至核心通过双链路上连核心，整网启用屏蔽双绞线（Shielded Twisted Pair，STP）防环。STP 在网络物理链路发生故障时网络收敛时间相对较长。整体网络在可扩展性、高可用性以及稳定性方面在智慧医院推进过程中逐渐显示出不足，因此迫切需要对整网进行改造。

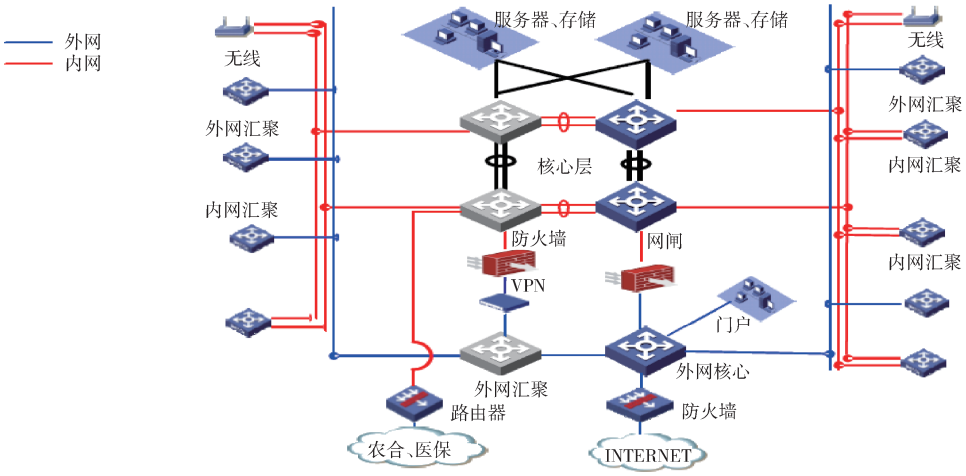

图 3　医院传统内外网物理隔离网络架构

3　多网融合网络架构

3.1　设计

遵循核心 - 汇聚 - 接入 3 层扁平化架构设计原则，内网、网外、设备网 3 网运行在同一套物理网络中，骨干间采用万兆互联。核心设备部署两台云计算数据中心核心交换机，双机虚拟化（IFR2）。楼宇汇聚层部署两台汇聚交换机做双机虚拟化，汇聚交换机采用双链路万兆至核心，分布式 VXLAN 网关部署在汇聚交换上通过 VXLAN 技术划分虚拟化专网，保证隔离强度，3 网互不影响，节省网络投资，接入层设备采用动态 VLAN 接入，通过 TRUNK 的方式采用双链路到汇聚层，汇聚层完成 VLAN 到 VXLAN 的映射。核心交换机旁挂部署控制器 AD Campus，核心和汇聚之间启用开放式最短路径优先协议（Open Shortest Path First，OSPF）保证 3 层互通，核心和汇聚之间启用 VXLAN 组网构建 Overlay 网络[3]。3 网在同一套物理网中，对人员按用户角色自动分配 IP 以虚拟隔离通道，获取相同网络权限，使医院内部终端在任意位置接入网络可获得相同权限以及用户业务随行、用户组安全隔离。VXLAN 多网络融合拓扑，见图 4。

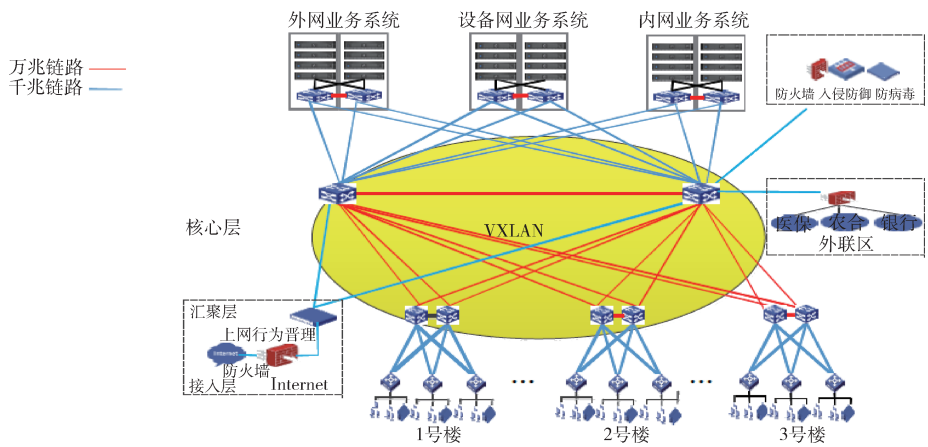

图 4　VXLAN 多网融合网络拓扑

3.2　网络资源策略管理

策略管理上采用面向业务的分组模式，将属性或访问权限相近的用户分到一个安全组中，同时也将服务器侧的资源划分到安全组进行统一管理。策略定义基于矩阵表格的方式简单直观，见表 1。具

体策略可简单可复杂。实现各种高级复杂的策略控制功能。根据用户分配 IP，用户名与 IP 地址一一对应，用户策略上采用面向业务分组的方式，将属性或访问权限相近的用户分到一个用户组中，同时也将服务器资源划分到相应的用户组进行统一管理，基于 5W1H 灵活用户认证接入机制，根据谁（who）、谁的设备（whose）、什么设备（what）、什么时间（when）、什么地点（where）、什么方式（how）多个维度覆盖各种接入场景。根据个人需求灵活定制场景，保障内网访问安全。网络访问策略定义，见表 2。

表 1 用户组及相关网络资源定义

用户组	5W1H 定义	网络属性	IP 组	隔离域
护士	护士站	VLAN10/VXLAN1	Ⅰ网段	VRF1
医生	医生站	VLAN20/VXLAN2	Ⅱ网段	VRF2
主任	不限	VLAN30/VXLAN3	Ⅲ网段	VRF3
行政	不限	VLAN40/VXLAN4	Ⅳ网段	VRF4
管理人员	不限	VLAN50/VXLAN5	Ⅴ网段	VRF5
……	……	……	……	……

表 2 网络访问策略定义

组别	临床组	医技组	后勤组	管理组	临床 Server	医技 Server	公共 Server	Interner
临床组	–	PERMIT	DENY	PERMIT	PERMIT	PERMIT	PERMIT	DENY
医技组	PERMIT	–	DENY	PERMIT	PERMIT	PERMIT	PERMIT	DENY
研发组	PERMIT	PERMIT	PERMIT	PERMIT	PERMIT	PERMIT	PERMIT	DENY
后勤组	DENY	DENY	–	–	DENY	DENY	PERMIT	PERMIT
管理组	PERMIT	PERMIT	PERMIT	PERMIT	PERMIT	PERMIT	PERMIT	PERMIT

3.3 网络虚拟通道隔离

汇聚和核心设备之间运行 VXLAN 构建 Overlay 网络，具备跨广域网的通道隔离能力，相比多协议标签交换（Multiple Protocol Label Switching，MPLS）的方式，VXLAN 隔离只需要在端点（VTEP）做隔离，不需要全网隔离。采用基于虚拟转发和路由（Virtual Routing and Forwarding，VRF）的方式替代传统的基于访问控制列表（Access Control List，ACL）的隔离，每个用户组在 VTEP 节点分配不同的 VRF，VRF 之间在路由层面实现隔离，每个用户在 VRF 内通过 VLAN 映射成不同的 VXLAN，最终在通道内经由 VXLAN 数据传输实现隔离，以此保障传输安全[4]。

4 成效

4.1 实现位址分离的网络架构

传统网络划分 L3 网段时通常和地理位置紧密关联，根据不同楼宇或楼层划分不同 L3 网段，当员工地理位置发生改变时往往跨越不同的 L3 网段会发生 IP 地址的变更从而丧失原有的权限，因此网络管理人员需根据新的 IP 重新调整对应的权限，针对该员工的策略控制也需做两套，增加网管的负担，也浪费交换机的 ACL 资源。通过 AD Campus 网络将 VXLAN 和 Overlay 技术结合实现柔性网络架构。使整体网络架构较灵活，业务部署（应用/终端）可以实现与地理位置无关[5]。无状态网络的核心实现位址分离，将用户分配的 IP 地址和实际地理位置解耦合，使 IP 地址可以在全网任意位置接入，不管用户移动到哪 IP 地址都能随身携带。IP 地址不仅能承担路由连通性的技术功能，还具有身份和业务的标识功能，达到用户无感无状态的效果。此网络结构下当员工地理位置发生变化时不需要分派两个地址，只需要一个固定 IP 地址即可，不管在哪个工位办公都可以使用，网管做策略时只要针对一个 IP 地址，工作量降低。对于分散在不同大楼的同部门员工可以分派同一个网段的地址，前缀相同，这样做策略时可以针对 IP 前缀做一条策略即可，避免逐个 IP 地址做策略。

4.2 实现用户策略随行

通常要实现策略随行需对用户进行分组，传统的分组方式受地理位置影响，与地理位置紧耦合。同一个用户组位于同一个办公区，通常很难跨越地理的局限。这样用户一旦移动起来策略实施就非常复杂，要达到策略跟随或者体验一致也非常困难。

将用户分组和 IP 网段严格对应，用户未入网前整个网络的策略控制内容已确定，通过采用名址绑定的方式为每个接入用户分配唯一的用户名，将用户名和 IP 地址一一对应。由于其本身提供无状态下任意位置访问功能，将用户名和 IP 地址绑定的功能相结合，当用户位置发生变化后，因 IP 地址和网段没有变化，所以针对 IP 的策略也未发生调整，这种针对 IP 的策略也是针对用户的策略，从而实现用户策略随行。

4.3 网随人动

通常医院网络终端根据最初的 IP 规划接入到相关接入交换机的端口，从而实现 VLAN 等权限和终端的匹配，不能解决用户和终端任意位置接入权限分配的问题，同时终端接入位置也受限制。AD Campus 网络将人和应用作为核心，所有网络资源跟随人和应用移动，用户在哪接入资源就下发到哪，真正体现柔性网络的网随人动特点[6]。

4.4 设备自动化部署

传统的网络上线需要网络维护人员为每台设备依次加电、更新版本、写配置、组网、调试和运行，逐台在核心、汇聚、接入配置。管理人员工作量大、冗杂而容易出错，网络上线时间较长。该网络架构中设备自动化部署得到极大简化，由于是无差别的网络，同样角色的设备配置基本相同，这样可以根据设备角色设定少量模板，一种角色的设备尽管数量很多，但由于共享同一个角色，因此使用一个配置模板，整网模板数量只有少量几种。设备加电后自动加载版本、配置，网管人员零干预启动。自动部署的核心是由于 AD Campus 网络将整网接入设备配置完全整合变成一份完全相同的配置文件，同时汇聚层设备也进行整合变成一份相同的配置。这大大简化配置文件编写的复杂度，使得各层次设备配置模板化，自动部署成本难度大大降低，同时也避免人为误操作风险，实现自动化部署，极大减轻网络管理人员工作负担。

5 结论

VXLAN 多网融合网络架构的核心技术支撑是在核心和汇聚之间构成的 L3 网络基础之上基于 VXLAN 技术构建 Overlay 网络。针对不同用户组对不同应用的访问创建不同 VXLAN 隧道，数据传输相互隔离，保障整体访问的安全性。基于 VXLAN 的医院多网融合技术架构有以下特点：一是降低投入成本，内网、外网、设备网络运行在同一物理网络上，无需部署多套硬件设备，减少网络硬件投入。二是更好地服务于临床，全网用户可以从任意位置接入，无需更改 IP 即可获取和以往相同访问权限，无需等待信息中心人员重新调整策略，给临床一线工作带来便利，从网络服务层面促进临床工作。三是运维简单化，整网核心、汇聚、接入各配置统一简化配置，新设备上线可实现自动部署，简化网络管理人员运维工作。四是智慧便民，构建高可用、易扩展、互联互通的多网融合网架结构有效保障医院临床应用系统的稳定性，及时有效地传输患者相关就诊及结算信息，减少给排队等待时间，给就诊带来便利。

目前基于 VXLAN 的网络融合技术在医疗信息化领域应用还不广泛，依托信息技术为基础的智慧医院离不开高可用、易扩展的基础网络为支撑。本文系统性地介绍 VXLAN 的技术原理和基于 VXLAN 多网融合网络架构研究与应用，是对目前 VXLAN 技术研究成果在医疗信息化领域应用的总结。基于 VXLAN 的多网融合技术对于打造互联互通、惠民、惠医、惠政的智慧医院有着至关重要的作用。

参考文献

1 钟耿辉. 基于 VXLAN 的 EVPN 技术研究与实现［J］. 计算机技术与发展，2017，27（5）：46－50.

2 姬凌宇. 软件定义网络 VXLAN 的研究与应用［J］. 延安职业技术学院学报，2017，31（5）：98－99.

3 张国平. 基于 SDH 和 Overlay 的云计算数据中心网络［J］. 中国新通信，2015（3）：109－111.

4 多伊尔（Jeff Doyle）. 卡罗尔（Jennifer Carroll）著，葛建立，吴剑章译. TCP/IP 路由技术（第 2 版）［M］. 北京：人民邮电出版社，2007：290－300.

5 何宇. 软件定义网络分布式控制平台的研究与实现［J］. 网络安全技术与应用，2014（12）：74－75.

6 黄韬. 软件定义网络核心原理与应用实践［M］. 北京：人民邮电出版社，2014：110－120.