doi: 10.7690/bgzdh.2015.06.018

基于 VLAN 技术的某局域网改造方法

邹　杨[1]，米　兰[1]，谢瑞莎[2]，王　卉[1]
（1. 中国洛阳电子装备试验中心，河南 济源 454650；2. 国家电网洛阳供电公司，河南 洛阳 471023）

摘要：为解决某科研局域网常出现广播风暴、病毒传播、黑客入侵等问题，提出一种基于 VLAN 技术的具体改造方案。通过分析计算机网络的拓扑结构，采用以 VLAN 技术为基础，三层交换、访问控制、流量控制、入侵检测等技术手段进行补充改进。结果表明：改造后的局域网络在一定程度上减少了网络流量，节约了网络带宽，降低了网络内主机负载，使信息网络的快速高效和安全可靠性能大大提高。

关键词：VLAN；ACL；三层交换；访问控制
中图分类号：TP393.02　　**文献标志码：**A

A Upgrading Research of Test LAN Based on VLAN Technology

Zou Yang[1], Mi Lan[1], Xie Ruisha[2], Wang Hui[1]
(1. *China Luoyang Electronic Equipment Test Center*, *Jiyuan* 454650, *China*;
2. *Luoyang Power Company of National Grid*, *Luoyang* 471023, *China*)

Abstract: For solving such network problems, like broadcast storms, viruses, hacking and even the virus spreading etc. This article presents a VLAN upgrading methods. By analyzing the topology of the computer network, use technology to VLAN-based, three-tier exchange, access control, flow control, intrusion detection and other technical means to complement improvements. The results show that after the transformation of the local area network to a certain extent, reduce network traffic and save network bandwidth and reduce network-host load, so fast and efficient, and the safety and reliability of information networks can greatly improve.

Keywords: VLAN; ACL; three-tier exchange; accessing control

0　引言

随着某科研机构建设发展，网络设备增多、规模扩大、流量突增，多阵地资源整合、联调协作的密切，对局域网络的即时性、高效性、可靠性要求越来越高；同时由于阵地分散、走线复杂与不同路由交换设备混用以及路由交换设备新旧、性能差异等因素，不同网段内部协议、技术人员对网络技术的掌握上的差异都可能导致网络问题的出现，如广播风暴、病毒传播甚至黑客入侵。针对本局域网存在的问题和VLAN[1]技术特点，笔者给出一种基于VLAN技术[2]的局域网改造设计方案。Cisc3550、Quidway3700和Quidway5700系列以太网交换机支持VLAN、多播过滤、三层交换[3]、访问控制等高级网络功能。在网络安全管理等策略配合的情况下可避免广播风暴、非法访问、网络扫描、黑客入侵和病毒传播等，从而在一定程度上节约了网络带宽、减少了网络流量、降低了网络内主机负载，提高了局域信息网络的即时性、高效性和安全可靠性。

1　网络改造需求分析

1.1　某科研中心原有计算机网络的拓扑结构

该中心局域网组建于 2006 年。目前有思科和华为 2 个品牌 4 个类型的交换机，主要以 Windows XP、Windows 2000 和 Windows Server 2003 为操作系统组成的大型局域网。因保密需要，整体网络未接入广域网，阵地 A、B、C 网络组均有类似的网络构成。近几年来，大量网络问题的爆发式出现，如广播风暴、病毒传播等，导致不同程度的通信中断、网络阻塞等，影响了试验的进行，甚至对研究结果产生不可忽略的干扰。该局域网原有计算机网络拓扑结构如图 1。

1.2　对网络改造的需求进行分析

科研局域网的设计应针对不同的应用需求，构造不同的应用子网，采用不同的网络接入技术和访问策略。对整个网络采用 VLAN 技术和交换技术，以使整个网络更加高效、可靠。

1.2.1　现有问题分析

1.2.1.1　结构方面

星形拓扑结构网络具有构造简单、控制方便和便于隔离的特点。但在该中心局域网中，由于需要接入局域网的节点较多(超过 200 个，并将继续增加)，距离分布较大，网络建设成本较高。部分节点距离交换机较远，信号衰减明显。由于网络在组建

收稿日期：2015-02-12；修回日期：2015-03-15
作者简介：邹　杨(1987—)，男，安徽人，学士，工程师，从事网络通信研究。

之初没有充分预料未来的发展变化，在局部工作域中模块较少。仅可使用小型交换机扩充容量，导致局部网络层次更加复杂，给故障排除带来较大困难。核心交换机承担了多数节点的数据交换工作，而且在任务期间网络负载突增，更使得核心交换机负担加重，造成网络拥塞的可能性增加。各区域间网络未隔离，各终端主机间可以互相访问，各区域数据的独立性、安全性无法保证。路由交换设备出现不同程度的老化现象，局域网与外阵地网络组之间缺乏有效的防火墙、入侵检测等设备。

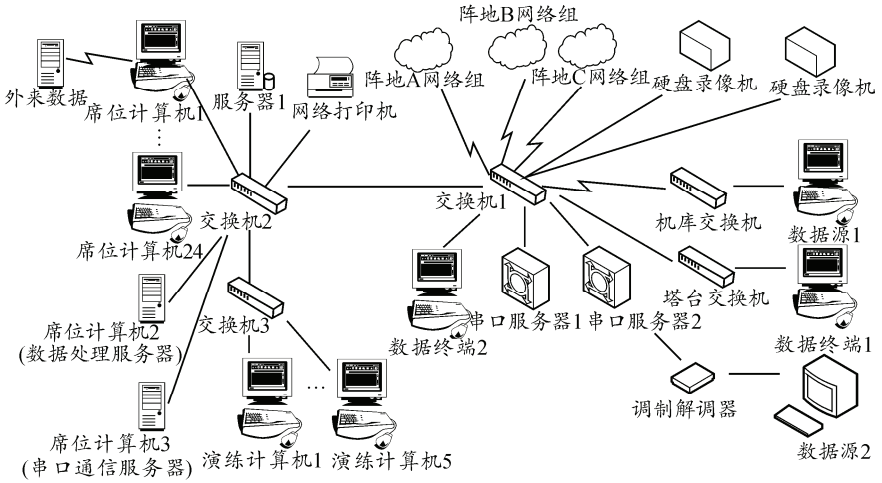


图 1　该中心原有计算机网络拓扑结构

1.2.1.2　组网策略方面

没有划分 VLAN。目前各个部门的网络并没有隔离，所有的网络设备可以互访，造成文件无法保密、病毒泛滥，一旦某单个节点出现问题，就可能造成整个网络的瘫痪。

1.2.2　解决方法分析

1.2.2.1　结构方面

由于核心交换机的承载压力巨大，故而应建立备用的交换机连接，以便当核心交换机发生故障时，网络能够快速切换到备用交换机上，从而保持正常通信。为保证物理上和外围网络组的安全连接，应更新路由交换设备；增加物理防火墙，以对网络病毒等起到一定的屏障作用。

1.2.2.2　组网策略方面

组网策略也是文中的重点。VLAN 主要作用是隔离广播域，实现专网专用。同时还有利于科学管理，各部门独自占用一个独立的 VLAN，整个 VLAN 可升级、可扩展。网络节点的增减，IP 地址的变动都需要 VLAN 技术的支持。

局域网是一个封闭的系统，它需要具有抗攻击特性和极强的安全保密性，一些研究数据和管理数据只能允许特定的网络节点访问。笔者利用 VLAN、ACL、网络安全技术来合理解决安全与开放的问题，同时网络的访问控制、VLAN 划分与观察镜像主机的设置等都要由特定的控制端来实现。基于图 1，根据该局域网设计要求，要求如下：

1) 核心交换机(华为 5700 交换机 1)需创建备用路由设备。

2) 数据源 1 通过 3 台交换机与席位计算机 3(串口通信服务器）相连，同时与其他计算机隔离。

3) 数据源 2 调制解调后经串口服务器通过 2 台交换机与席位计算机 3(串口通信服务器)相连，同时与其他计算机隔离。

4) 席位计算机 2(数据处理服务器)通过 3 台交换机与数据终端 1、数据终端 2 互连，同时将数据终端 1、数据终端 2 互相隔离同时和其他网络隔离，且连接为单向通信。

5) 演练计算机 1 至演练计算机 5 内部互连，与外界隔离，只在特殊情况下和外界联通。

6) 阵地 A、B、C 网络组通过 3 台交换机仅与席位计算机 15 相连，16 备用。

2　工程实现

2.1　三层交换机的工作原理

交换机工作在 OSI 参考模型的数据链路层上，主要有网络拓扑结构、物理编址、帧序列、错误校验以及流量监控的作用。三层交换机[4]实质就是一种特殊的路由器，在性能上侧重于交换(二层和三层

之间)，有很强交换能力且价格低廉的路由器。它将第2层交换机的交换功能和第3层路由器的路由功能加以结合，可在2个层次增加线速性能。该结构还具有策略管理的作用，它不仅使得第2层与第3层相关联，同时还具有流量优先处理、网络安全策略等多种灵活的功能，如VLAN、链路汇聚和Intranet的动态部署[5]。三层交换机的结构分为接口层、交换层和路由层三层结构[6]。

2.2 局域网VLAN规划及设置

当前，该中心局域网的构造方式是将网络环境所有的计算机都全部规划为一个网络，这种星型网络结构不够稳定、安全性差、容易产生广播风暴和病毒传播。为解决上述问题，就必须对该局域网络进行重新设计。利用现有的路由交换设备对内网地址的VLAN进行划分，规划对交换网络使用的访问。

根据该局域网设计要求，设计虚拟局域网如下：

1) VLAN 10：192.168.126.0/28为核心交换机(华为5700交换机1)子网。交换机网关设置为192.168.126.3，防火墙IP地址设置为192.168.126.4。同时为核心交换机建立路由冗余机制。

2) VLAN 20：192.168.127.0/24为服务器子网。网关设置为192.168.127.3，各客户机IP设置为192.168.127.4以后。网段内的计算机都可以共享服务器的信息。

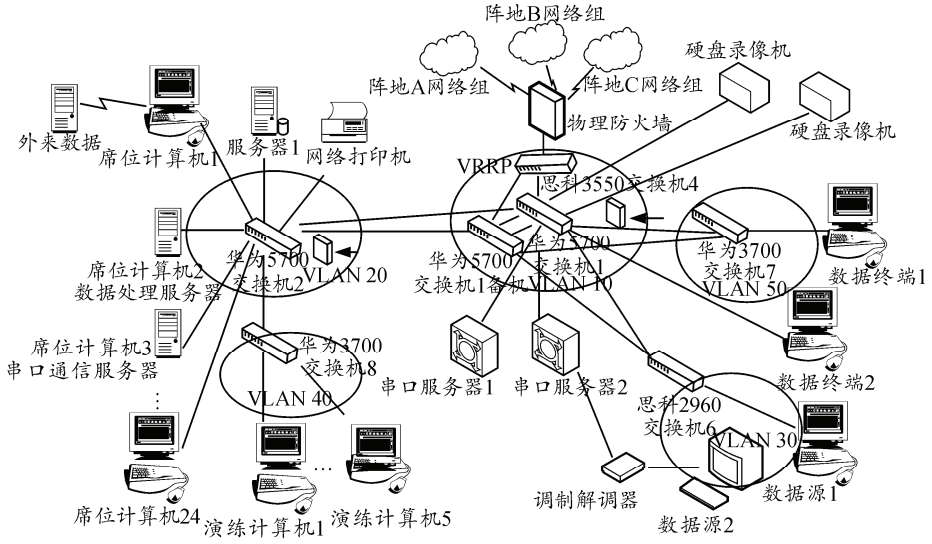
3) VLAN 30：192.168.128.0/24为数据源子网。网关设置为192.168.128.3，各客户机IP设置为192.168.128.4以后。数据源1和数据源2通过加入隔离组1实现相互隔离，且仅与席位计算机3(串口服务器)通信。

4) VLAN 40：192.168.129.0/24为演练计算机子网，网关设置为192.168.129.3，各客户机IP设置为192.168.129.4以后。建立高级ACL，实现服务器信息被此子网共享。

5) VLAN 50：192.168.130.0/24为数据终端子网，网关设置为192.168.130.3，各客户机IP设置为192.168.130.4以后。两数据终端计算机通过加入隔离组2实现相互隔离，建立三层交换和高级ACL使得席位计算机2(数据处理服务器)可访问这2个数据终端计算机。

通过以上配置，每个独自的工作区域都归属于不同的子网，每个子网的可用地址数为13个或253个，可解决各区域因网络节点增加网络地址不足的问题。区域内部计算机之间的访问不受限制，而区域之间的网络访问则需通过设置三层交换机来实现，从而实现了局域网络、向多层次、路由型网络结构的转变。这样做有助于使不同子网之间实现隔离，没有业务联系的区域之间网络不能相互访问，需要进行业务联系的区域通过在交换机上设置IP访问控制协议，杜绝了单个子网内的病毒传播到整个网络，确保了各VLAN区域内专有数据的安全；此外还便于扩展，新的网络规划里给各局域网区域预留了充足的IP地址空间，使得区域内网络地址的规划具有可持续性和统一性。

因阵地A、B、C网络组是外接入网络，故而应建立一个防火墙，以起到入侵检测、信息过滤与防范病毒方面的作用。按照规划，设计如图2。



注：图中双连线表明与交换机1、备用交换机都有同样连接

图2 该中心改造后计算机网络拓扑结构

2.3　交换机配置关键指令

2.3.1　异构交换设备间 VLAN 互通的根本原则[7]

针对该中心局域网的具体路由交换设备情况，有思科和华为 2 种类型的交换机，因此必须要将所有 Trunk 端口都定义成 IEEE802.1Q[8]协议。在 VLAN 信息的管理和配置上，VTP[9]和 GVRP 协议都是被思科设备支持的协议，而华为设备支持 GVRP 协议。因此在采用 GVRP 协议的情况下，各路由设备可从GVRP协议服务器学习到VLAN信息。

2.3.2　网络设备配置关键 ISO 命令

2.3.2.1　在核心交换机上配置 VRRP 协议

在华为 5700 交换机 1 上

```
<Quidway> system-view
 [Quidway] sysname RTA
 [RTA] interface Ethernet 0/0
 [RTA-Ethernet0/0] ip address 192.168.126.251 28
 [RTA-Ethernet0/0] vrrp vrid 1 virtual-ip 192.168.126.254
```

在华为 5700 交换机 1 备机上

```
<Quidway> system-view
 [Quidway] sysname RTB
 [RTB] interface Ethernet 0/0
 [RTB-Ethernet0/0] ip address 192.168.126.252 24
 [RTB-Ethernet0/0] vrrp vrid 1 virtual-ip 192.168.126.254
 [RTB-Ethernet0/0] vrrp vrid 1 priority 200
```

2.3.2.2　思科设备配置 VLAN Trunks

```
Switch# configure terminal
Switch(config)# interface fastetherne2/4
Switch(config—if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dotlq
Switch(config—if)# end
```

2.3.2.3　GVRP 配置

```
[SWA] vlan10 20
[SWA] gvrp
[SWA] interface Etherent 0/0/4
[SWA- Etherent 0/0/4] port link-type trunk
[SWA- Etherent 0/0/4] port trunk permit vlan 10 20 40
[SWA- Etherent 0/0/4] gvrp
```

2.3.2.4　创建 VLAN 及所属端口

```
[SWA-VLAN20] port GigabitEtherent 0/0/1 to 0/0/22
```

2.3.2.5　配置 Trunk 端口

```
[SWA] interface GigabitEtherent 0/0/23
[SWA- GigabitEtherent 0/0/23] undo port default vlan
[SWA- GigabitEtherent 0/0/23] port link-type trunk
[SWA- GigabitEtherent 0/0/23] port trunk allow-pass vlan 10 20 40
```

2.3.2.6　配置端口隔离

```
[SWA] interface GigabitEthernet 0/0/5
[SWA- GigabitEthernet 0/0/5] port-isolate enable
[SWA- GigabitEthernet 0/0/5] quit
[SWA] interface GigabitEthernet 0/0/6
[SWA- GigabitEthernet 0/0/6] port-isolate enable
```

2.3.2.7　建立访问控制（以华为交换机配置为例）

创建高级 ACL 列表如下：

```
[RTA2] Firewall enable
[RTA2] acl number 3001
[RTA2] rule 5 permit ip source 192.168.128.2 0 destination 192.168.127.5 0.0.0.0
[RTA2] rule 6 permit ip source 192.168.128.3 0 destination 192.168.127.5 0.0.0.0
[RTA2] firewall packet-filter 3001 inbound
```

在图 2 所示的华为 5700 交换机 2 上应用高级 ACL 方法，可以有效地控制流量，控制访问许可，达到控制网络访问的目的。

2.4　改造后的网络测试效果

通过模拟仿真软件运行，运行效果得到大幅提升。通过 VLAN 技术的应用，网络通信从以太网方式变为点到点方式，有利于控制广播域和网络流量，加强网络的安全性；同时将不同局域网区域隔离，可以实现区域间共享资源的访问限制，控制各个区域子网之间的互访，杜绝非法访问。此外，通过建立物理防火墙、路由冗余机制、流量控制等手段，隔离了外部网络可能存在的干扰，使核心的网络连接可靠性得到保障，增强了网络的安全性、健壮性、高效性。

3　总结

笔者简要介绍了 VLAN 技术，针对该中心局域网存在的问题阐述了实施 VLAN 的必要性；并依据 IEEE802.1Q 标准阐述了 VLAN 的工作机制。笔者以该中心局域网改造为例，从网络性能、可扩充性、

用户管理、安全性等方面对网络结构进行了分析。结合具体要求，笔者提出了针对该局域网的解决方案：包括 VLAN 的划分、端口隔离、访问控制等，进行了网络改造，使局域网络有了质的飞跃，提高了该中心的通信保障能力。

参考文献：

[1] 车保霞. VLAN 技术研究及其在校园网中的实现[D]. 成都: 电子科技大学, 2005.

[2] 洪军, 韩燮. VLAN 技术及在交换机上的实现[D]. 太原: 中北大学, 2007.

[3] Vito Amato. Cisco Systems Networking Academy[M]. 北京: 人民邮电出版社, 2002: 189-199.

[4] 仇剑锋. 基于 VLAN 和三层交换的企业网络安全策略研究[D]. 长沙: 中南大学, 2006.

[5] 李俊. 拒绝服务攻击的分析和研究[J]. 电脑与信息技术, 2002(6): 13-14.

[6] 骆珍, 裴昌幸, 朱畅华. DDoS 攻击的技术分析与防御策略[J]. 电子科技, 2006(12): 15-16.

[7] 左明慧, 冯乐. 混合组网环境下 VLAN 互通问题及实现[J]. 苏州科技学院学报, 2007, 24(2): 77-80.

[8] IEEE std IEEE802.1Q[1]-1998. IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks[S].

[9] 周剑岚, 冯珊, 孙建军. 守住最后一道防线: 文件过滤驱动程序在系统安全中的研究与应用[J]. 计算机安全, 2005(6): 12-15.

****

（上接第 55 页）

而我国也正在开展含能材料物化性能的研究，开展快速粘结及固化技术、增材制造过程安全控制与评价及产品质量综合测试等技术的研究，期待能够创新国内弹药装药及成型工艺，保障我国新型战略武器和先进常规战斗部实现目标高效毁伤的可靠性，为我国高新武器弹药高效毁伤技术研究提供新方法，为未来新型武器装备研制与生产提供新工艺和新装备，实现小药量、复杂异性战斗部的高密度一致性、无内部疵病、低空隙率装药。

参考文献：

[1] 陈道君, 姜联成, 范玉德. 含能材料机械加工安全控制技术[J]. 含能材料(增刊), 2004, 12(11): 629-632.

[2] 孙国光. 三维打印快速成型机材料的研究[D]. 西安: 西安科技大学, 2008.

[3] 邢宗仁. 含能材料三维打印快速成形技术研究[D]. 南京: 南京理工大学, 2012.

[4] Hon K K B, Li L, Hutching I M s. Direct writing technology-Advances and developments[J]. CIRP Annals-Manufacturing Technology, 2008: 601-620.

[5] 王建. 化学芯片的喷墨快速成型技术研究[D]. 南京: 南京理工大学, 2006.

[6] Robert A. Fletchera, Jacquelyn A. Brazin, Matthew E. Staymates, etc. Fabrication of polymer microsphere particle standards containing trace explosives using an oil/water emulsion solvent extraction piezoelectric printing process[J]. Talanta, 2008: 949-955.

[7] 朱锦珍. 含能芯片的快速成型技术研究[D]. 南京: 南京理工大学, 2005.

[8] 宋健康. 快速成型技术在引信中的应用[D]. 南京: 南京理工大学, 2005.

[9] 付尧, 冯清秀. 基于DSP的三维打印机控制系统研究[J]. 机电工程, 2014, 31(2): 217-220.