

广东电大省校校区网络升级方案^{*}

乐 军

(广东广播电视大学网络中心, 广东 广州 510091)

摘 要: 介绍了广东电大省校校区网络升级的设计与实现, 千兆以太网与第三层交换的技术的应用与 Alcatel 产品的实现, 以及 Vlan 技术与基于包过滤的安全策略在校园网中应用。

关键词: 千兆以太网; 第三层交换; Vlan; 网络管理

中图分类号: TP393.18 **文献标识码:** A **文章编号:** 0529-6579 (2002) S1-0007-03

广东广播电视大学省校校区在 1997 年建成了采用 100M 快速以太网技术的校园网, 以 64K DDN 的方式接入 Cernet。当时仅有 260 多台机接入, 两栋教学大楼之间使用光缆连接。目前接入的主机有 800 多台, 子网增加到 14 个之多, 形成了一个中等规模的园区网, 而且新建成的一栋综合大楼需要接入校园网。一些如网上直播课堂、基于 WEB 的远程教学、基于 ASP 方式的管理系统等新的业务需要开展。原有的网络难以应付新的办学需要, 反映在主干与接入 Cernet 的带宽不足, 原有主干交换机难以承担传输的任务, 子网间通过 NT Server 实现的路由传输效率低, 新楼需要接入校园网, 整个校园网需要进行升级。

1 网络建设的目标与升级的原则

校园网建设的目的是贯彻落实国家“科教兴国”战略, 推进广东广播电视大学的信息化建设, 为我省电大系统的远程开放教育提供一个良好的通信平台。其长期目标是建设一个连接市县电大的高速宽带的计算机网络, 中期目标是建成连接广州市几个分校的城域网, 近期目标是提高校园网主干与接入 Cernet 的速率。

基于资金、技术、人员与应用等因素的影响, 它不可能一步到位, 而是一项长期的工作, 在策略上要统一规划, 分步实施。在原则上校园网应具备先进性、可靠性、开放性、扩充性、安全性、实用性、可维护性。技术的先进性将保证整个网络系统高效率、稳定可靠地运行, 应该选

用先进主流的技术与设备来满足校园网的业务需求; 通过良好的网络结构, 主干线路、网络核心设备、服务器和电源的冗余备份来保证网络运行的可靠性, 避免因局部的故障而引起整个网络的瘫痪; 网络系统应符合国际标准, 提供开放的网络接口, 系统易于升级和功能扩充, 以便保护原有的投资; 网络的功能应该立足于满足一定时期内学校教学与管理的需求, 选用的系统设备技术具有较高的性能价格比; 能够提供有效的网络管理和系统监控技术, 保证系统维护管理简单方便; 网络系统与网络信息具有高度的安全性和保密性, 通过 VLAN、用户认证、代理、防火墙等来确保网络的安全^[1-3]。

2 网络主干的技术方案

2.1 网络主干技术

当前园区网的主干技术主要有 ATM 与千兆以太网两种, 要根据多方面的因素来考虑选用何种技术。ATM 采用了信元传输和交换技术, 在减少时延与服务质量保证 (QoS), 按需划分带宽, 实现语音、数据与视频混合传输方面有较好的性能, 但它更多地是面向广域网的传输与大型综合网络。

随着千兆网技术的成熟, 越来越多的园区网采用了千兆以太网技术。因为它使用了与 10-Mbps 以太网相同的帧格式和帧大小以及相同的 CSMA/CD 协议, 无需增加附加协议栈或中间件就可以进行平滑升级, 包括从交换机到交换机、交换机到服务器、交换机到路由器的连接, 从而

* 收稿日期: 2002-03-21

作者简介: 乐 军 (1964-), 男, 副教授; E-mail: lejun@gdrtvu.edu.cn

实现从快速以太网无缝升级到千兆以太网。千兆以太网增加了 IGMP 的 IP 组播、IEEE802.1P 标准、IEEE802.1Q 标准的 VLAN 管理策略、COS/QoS、RSVP 等服务功能。它还继承了传统以太网管理简单的特点, 增加的管理成本较少。目前主流的千兆交换机支持第三层、第四层交换, 实现线速的路由交换。

基于以太网的优点与校园网多媒体应用情况, 以及原校园网是快速以太网与升级后接入采用千兆以太网技术的广东教科网的城域网等因素考虑, 我校采用了千兆以太网与第三层交换的升级技术方案。

2.2 网络结构与设备选型

为了今后网络的扩充与安全管理, 把校园网分为广域网、主干网、局域网三个层次。广域网部分是指校园网与 GDERNET/CERNET 的互联, 主干网是把网络中心所在的教学楼与电教大楼、综合楼用 8 芯的室外多模光纤连接起来, 大楼内各个部门的局域网用超五类双绞线接入楼内的主干节点, 形成三级的网络结构, 10M/100M 交换到桌面。

边界路由与主干交换机采用了四台 Alcatel 的 OC5010 路由交换机; 二级交换机采用 Alcatel 的 OS5024、OS4024C 交换机, 通过超五类线与 OC5010 上联, 同时下接局域网的其它交换机或

工作站; 校园网边界路由交换机 OC5010 通过 100M 的 Tx 端口用超五类线与放在我网络中心的 GDERNET 汇接点的一台 OC5010 相联, 其中汇接点的 OC5010 是通过中国网通城域网的 100M 的数据链路与省网骨干接点教育厅相连。校园网的拓扑结构如图 1 所示。

2.3 网络设备的主要性能

校园网主干交换机 OC5010 支持 3 层交换, 有 20 个 10/100Base Tx 端口, 2 个 1000 Base SX 千兆以太网端口, 提供近 6 百万包/秒的线速路由, 支持 256000 条第二层和第三层路由容量, 支持 IEEE802.3u、IEEE802.3ad、IEEE802.3z、IEEE802.1D、IEEE802.1p、IEEE802.1Q、BGP、BGP-4、RSVP、RMON2 等协议, 整个设备的性能满足学校目前教学等需求。

3 网络安全与管理

3.1 基于 Vlan 的网络管理

由于主要的交换机均支持 802.1Q 的标准, 因此在校园网中应用 Vlan 技术来实现对整个网络的安全和灵活的管理。以实用性、灵活性、安全性、效率性与应用性为原则, 把业务性质相同的部门划分到同一个 Vlan, 隔离了不同部门的 IP 地址, 防止了 IP 的盗用与广播风暴, 提高网络的传输效率。划分的策略有: Port, MAC,

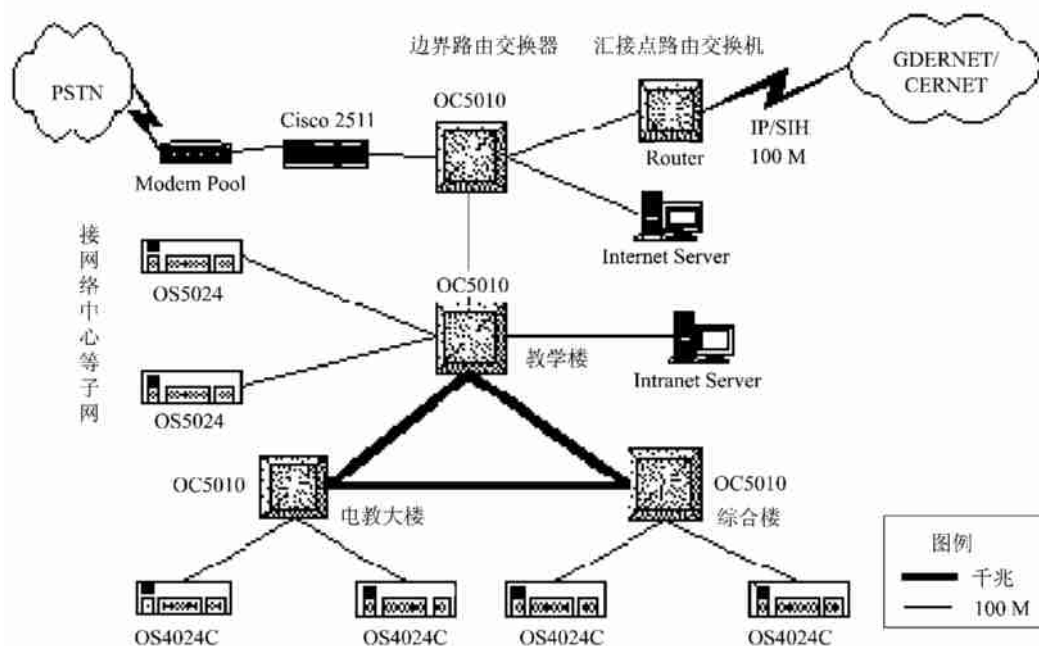


图 1 校园网的拓扑结构

Protocol, Network Address, Port Binding, User Defined 等，其中 Port Binding 的策略主要有：Port+IP+MAC, Port+MAC+Protocol, Port+Protocol, IP+MAC, IP+Port, Port+MAC。在主干 OC5010 上主要采用了 Port+IP 的划分策略，同时设定 Vlan 的优先级来确保多媒体传输的需要。在局域网这一层，主要采用 Port+IP+MAC、IP+MAC、Port+IP 的绑定策略来提高网络的安全性。网管软件 Track View 与 X Vision 提供了网络管理的图形化的界面，减轻了网管工作的负担。

3.2 网络安全控制

校园网采用了包过滤与代理服务的安全策略。OC5010, OS5024 对数据包的两种类型 “In” 与 “Out” 可以设置 “Allow” 与 “Block” 的策略，支持面向 Vlan 的包过滤。在校园网这 4 台的 OS5010 与 2 台 OS5024 上灵活应用这过滤策略，对不同的 Vlan 来设置不同的过滤规则，如在教学实验室仅开放国内的 IP 地址，内部办公服务器仅提供给校内的 IP 使用，在边界路由上则滤掉一些不安全的 IP 等。

在交换机的安全方面，Alcatel 的这几个类型的交换机均支持基于 Ftp、Telnet、Tftp、Snmp、Http 协议的用户的安全访问控制。可以开设三个不同权限层次的用户，具有完全控制权的 admin 用户，具有部分读写权的用户，仅有一般读权限的用户，列表中的用户可以采用 Radius 服务器来认证。通过 Access List 控制列表，指定能够访

问的 IP 地址、MAC 地址、端口号等。对于校园网的主干交换机，为了安全可以关闭了一些服务，如 Telnet, Ftp, Tftp 等，仅通过网管软件进行监控。对一些需要开设的服务，仅允许个别的 IP+MAC+认证用户来进行访问，并定义好其口令的长度模式（口令的长度可以长达 80 个字符）。使用链路聚合的功能，把交换机的多个端口连接成为一个逻辑端口，最多可以支持到 4 个 100M 的全双工的端口连接，既增加了带宽又增加了线路的冗余备份。在局域网接入主干交换机中，用两个端口的聚合方式来提高冗余的能力。

4 结束语

通过以上的的工作，采用了三层交换与千兆以太网技术的校网络升级工程基本完成，增加了主干网络的带宽与传输的效率，提高了安全性与可靠性。以 100M 接入了 GDernet 的城域网，大大地提高了我校接入 Cernet 的带宽，为省校与各个市级分校通过省教科网实现高速的互联打下了坚实的基础。

参考文献：

[1] Andrew S. Tanenbaum. 计算机网络[M] . 第三版. 熊桂喜等译. 北京: 清华大学出版社, 1998
[2] Chris Hare, Karanjit Siyan. Internet 防火墙与网络安全 [M] . 刘成勇等译. 北京: 机械工业出版社, 1998.
[3] Http: //www. alcatel. com

The Upgrading Design of the Campus Network of GDRTVI

LE Jun

(Network Center, Guangdong Radio &TV University, Guangzhou 510091, China)

Abstract: It introduces the upgrading design and implementation of the campus network of GDRTVU, which applied Gigabit Ethernet and layer 3 switch in the backbone, Alcatel products, and the network management policies based on Vlan and ip packet filter to the campus network.

Key words: gigabit ethernet; layer 3 switch; vlan; network management