

文章编号: 1005-8451 (2006) 08-0045-03

基于 VLAN 技术的校园网安全研究与应用

吴献文¹, 毛春丽², 肖立权³

(1. 湖南铁道职业技术学院 信息工程系, 株洲 412001; 2. 湖南商学院 艺术设计系, 长沙 410205;
3. 国防科学技术大学, 长沙 410073)

摘要: 以湖南铁道职业技术学院的校园网为背景, 从校园网的特点和传统局域网技术入手, 研究了 VLAN 技术在校园网安全中的应用。

关键词: VLAN 技术; 校园网; 网络安全; 研究

中图分类号: TP309

文献标识码: A

Study and application of campus network security based on VLAN technology

WU Xian-wen¹, MAO Chun-li², XIAO Li-quan³

(1. Department of Information Engineering, Hunan Railway Professional-Technology College, Zhuzhou 412001, China; 2. Department of Art Design, Hunan Business College, Changsha 410205, China;
3. National University of Defense Technology, Changsha 410073, China)

Abstract: Based on the background of Hunan Railway Professional Technology College, the feature of Campus Network and the VLAN technology, it was researched the application of VLAN in this thesis according to the safe demands of the Campus Network.

Key words: VLAN technology; campus network; network security; research

随着 Internet 技术、网络技术、信息技术、多媒体技术的迅猛发展, 校园网已经成为学校教学、科研、管理和信息获取的重要手段。但是, 校园网访问方式多、用户群庞大、网络行为突发性高, 为了保证校园网的正常运行和安全, 本文主要针对校园网的特点和传统局域网的缺陷, 重点介绍了基于 VLAN 技术构建安全校园网的应用。

1 校园网络特点分析

校园网对于提高教学和科研质量、加快学校信息化建设、开展多媒体教学与研究、改善教学和科研条件有着十分重要的意义。

校园网络大, 故障定位复杂, 维护难度大。由于教学逐步走向网络化、多媒体计算机教学越来越普及、学生在线学习和娱乐时间增加, 要保证校园网稳定可靠, 必须 7*24 h 正常和高效运行, 因此网络维护只能利用比较空闲、相对流量较小的时间段。

校园网用户群密集, 网络安全问题蔓延快、对网络影响严重。某台计算机由于各种原因出现故

障, 反过来又会影响整个网络。

校园网业务多, 开放性强, 是教学、科研的特定场所, 也是新技术、新知识最先应用的场所, 网络环境相对比较宽松。因此安全隐患比较大。

校园网管理难度大, 计算机购置和配置情况复杂。

随着每个端口以太网和令牌环网的交换机价格下降, 为了获得更高的带宽, 越来越多的学校和组织倾向于给每个用户分配一个单独的交换端口。

校园网的使用引起了教学方法、教学手段、教学工具的重大革新。为学校管理者和老师提供了获取资源、协同工作的有效途径, 是教育信息化发展不可或缺的工具。校园网安全、高效运行是每个校园网信息获取和教学的保障, 在校园网中采用新兴技术迫在眉睫。

2 VLAN 技术

VLAN 技术是在局域网内将工作站逻辑的划分成一个个网段, 从而实现虚拟工作组的技术。

基于交换网络的 VLAN 目前大致可分为 4 类: 基于端口的 VLAN (见图 1、图 2)、基于 MAC 地址的 VLAN、基于路由的 VLAN 和基于策略的 VLAN。基

收稿日期: 2006-05-09

作者简介: 吴献文, 在读硕士研究生; 毛春丽, 在读硕士研究生。

于端口的 VLAN 划分是最简单、最有效的划分方法,是基于交换机端口的划分方法,只需网络管理员对网络设备的交换端口进行重新分配,不需考虑该端口所连接的设备,就可将属于不同交换机端口的不同网段划分在一个 VLAN 中;基于 MAC 地址的 VLAN 是 MAC 地址的集合,允许网络用户从一个位置移动到另一个物理位置,且自动保留起所属 VLAN 的成员身份,是基于网络用户的,但由于 MAC 地址的唯一性,初始化困难,且网卡更换就必须重新配置,另外它不能防止 MAC 欺骗攻击,有可能受到假冒 MAC 地址攻击的危险。

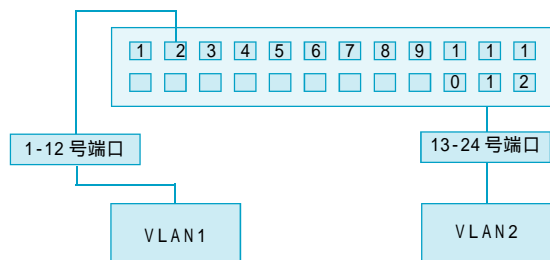


图 1 同一交换机的端口划分到不同的 VLAN

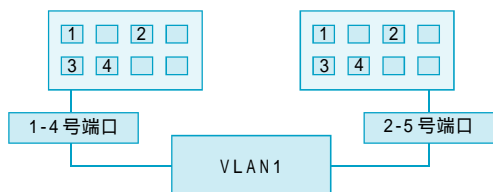


图 2 不同交换机的端口划分到同一 VLAN

VLAN 技术的出现为网络设计、扩展、更改提供了更大的灵活性,主要体现在如下:

(1) 提高网络设计的灵活性。

(2) 方便站点的移动、增加和变化,大大提高管理动态网络的能力。

(3) 提高网络安全功能。VLAN 与 VLAN 间逻辑上是分开的,VLAN 成员的数据包只能在同一 VLAN 内部传送,即使处于同一网络中,不同 VLAN 间也不能进行直接通信,有效地避免了广播风暴的传播;校园网中,如财务管理、人事档案管理及一些不对外公开的科研数据资料库等应用系统,网络管理员可采用 VLAN 技术对广播域进行逻辑划分,达到限制用户非法访问的目的,从而确保重要部门的数据安全。除非设置了监听口,信息交换就不可能存在监听和插入问题,提高了网络的安全性能;对于内网,采用基于 MAC 地址的 VLAN 技术,可有效防止 IP 地址盗用问题。

(4) 采用 VLAN 技术的网络中,每个 VLAN 内的站点可直接访问该 VLAN 内的服务器,提高了网络的响应速度;同时,同一个 VLAN 内的站点可以非常方便的进行通信。

(5) 简化网络管理。VLAN 是一个在物理网络上根据用途、工作组、应用等来逻辑划分的局域网络,与用户的物理位置没有关系。采用 VLAN 技术,网络管理员只需设置指令就能为某个项目或任务建立 VLAN。

3 VLAN 技术在我校校园网中的应用

3.1 校园网情况介绍

(1) 出口:学校与电信的网络接口带宽为 100 MB,与教育网的网络接口带宽为 64 KB;(2)域名: hnrpc.com;(3) IP 地址范围: 218.75.196.218-----;(4)中心交换机: CISCO 3550。

目前,校园网覆盖的楼包括:图书馆、办公楼、各校区教学楼、实验楼和多媒体中心。学生宿舍楼没有介入校园网,由电信负责接入。

3.2 学校系统情况

目前,学校运行的系统主要为:Web 服务器一台;流媒体服务器一台;图书管理系统;财务系统。就网络整体结构而言,我校校园网是一个千兆和百兆以太网链路连接的园区网络。整个网络根据范围的限制可分为两个大的部分:内网和外网。从网络安全级别的角度考虑又可将内网分为两大部分:第 1 部分为重点信息安全保护区,即校园网的重要应用服务器群和重要部门的网络设备和用户;第 2 部分为普通信息安全区,即校园网中普通应用的网络设备和用户。外网即为校园外部网络区域,也就是与校园网相连的教育网和 Internet。校园网重点考虑网络内部安全:信息访问安全和物理安全。信息访问安全即为内部网络各部门和用户之间要能相互进行信息交换,又要保护重要部门数据的保密性,同时应禁止外部用户非法访问内部数据。

3.3 校园网系统规划

(1) 安全技术:根据校园网的具体情况,为了达到信息流量的控制,并提供良好的安全性,通过对网络逻辑结构进行分析和合理划分,采用基于端口 VLAN 技术对校园内部网络不同部门之间进行逻辑隔离,同时抑制广播风暴。根据学校具体建筑物分布情况,每栋楼设置为一个 VLAN,共设置 10 个,

文章编号: 1005-8451 (2006) 08-0045-03

基于 VLAN 技术的校园网安全研究与应用

吴献文¹, 毛春丽², 肖立权³

(1. 湖南铁道职业技术学院 信息工程系, 株洲 412001; 2. 湖南商学院 艺术设计系, 长沙 410205;
3. 国防科学技术大学, 长沙 410073)

摘要: 以湖南铁道职业技术学院的校园网为背景, 从校园网的特点和传统局域网技术入手, 研究了 VLAN 技术在校园网安全中的应用。

关键词: VLAN 技术; 校园网; 网络安全; 研究

中图分类号: TP309

文献标识码: A

Study and application of campus network security based on VLAN technology

WU Xian-wen¹, MAO Chun-li², XIAO Li-quan³

(1. Department of Information Engineering, Hunan Railway Professional-Technology College, Zhuzhou 412001, China; 2. Department of Art Design, Hunan Business College, Changsha 410205, China;
3. National University of Defense Technology, Changsha 410073, China)

Abstract: Based on the background of Hunan Railway Professional Technology College, the feature of Campus Network and the VLAN technology, it was researched the application of VLAN in this thesis according to the safe demands of the Campus Network.

Key words: VLAN technology; campus network; network security; research

随着 Internet 技术、网络技术、信息技术、多媒体技术的迅猛发展, 校园网已经成为学校教学、科研、管理和信息获取的重要手段。但是, 校园网访问方式多、用户群庞大、网络行为突发性高, 为了保证校园网的正常运行和安全, 本文主要针对校园网的特点和传统局域网的缺陷, 重点介绍了基于 VLAN 技术构建安全校园网的应用。

1 校园网络特点分析

校园网对于提高教学和科研质量、加快学校信息化建设、开展多媒体教学与研究、改善教学和科研条件有着十分重要的意义。

校园网络大, 故障定位复杂, 维护难度大。由于教学逐步走向网络化、多媒体计算机教学越来越普及、学生在线学习和娱乐时间增加, 要保证校园网稳定可靠, 必须 7*24 h 正常和高效运行, 因此网络维护只能利用比较空闲、相对流量较小的时间段。

校园网用户群密集, 网络安全问题蔓延快、对网络影响严重。某台计算机由于各种原因出现故

障, 反过来又会影响整个网络。

校园网业务多, 开放性强, 是教学、科研的特定场所, 也是新技术、新知识最先应用的场所, 网络环境相对比较宽松。因此安全隐患比较大。

校园网管理难度大, 计算机购置和配置情况复杂。

随着每个端口以太网和令牌环网的交换机价格下降, 为了获得更高的带宽, 越来越多的学校和组织倾向于给每个用户分配一个单独的交换端口。

校园网的使用引起了教学方法、教学手段、教学工具的重大革新。为学校管理者和老师提供了获取资源、协同工作的有效途径, 是教育信息化发展不可或缺的工具。校园网安全、高效运行是每个校园网信息获取和教学的保障, 在校园网中采用新兴技术迫在眉睫。

2 VLAN 技术

VLAN 技术是在局域网内将工作站逻辑的划分成一个个网段, 从而实现虚拟工作组的技术。

基于交换网络的 VLAN 目前大致可分为 4 类: 基于端口的 VLAN (见图 1、图 2)、基于 MAC 地址的 VLAN、基于路由的 VLAN 和基于策略的 VLAN。基

收稿日期: 2006-05-09

作者简介: 吴献文, 在读硕士研究生; 毛春丽, 在读硕士研究生。