

本文引用格式: 李晋峰.虚拟局域网 IP 地址访问控制方法研究[J].自动化与信息工程,2022,43(4):18-21.

LI Jinfeng. Research on IP address access control method of virtual local area network[J]. Automation & Information Engineering, 2022,43(4):18-21.

## 虚拟局域网 IP 地址访问控制方法研究

李晋峰

(长治职业技术学院, 山西 长治 046011)

**摘要:** 针对当前虚拟局域网的控制方法在实际应用中受访问用户数量的影响, 导致控制准确率和耗时无法达到预期要求的问题, 开展虚拟局域网 IP 地址访问控制方法研究。通过局域网 IP 地址定位、用户身份识别和 IP 地址访问控制, 提出一种针对虚拟局域网的访问控制方法。通过对比实验证明, 本文提出的控制方法在有效提高访问控制准确率的前提下, 可缩短控制耗时, 促进虚拟局域网运行效率的全面提升。

**关键词:** 虚拟局域网; IP 地址; 访问控制; 用户身份识别

中图分类号: TN391

文献标识码: A

文章编号: 1674-2605(2022)04-0004-04

DOI: 10.3969/j.issn.1674-2605.2022.04.004

## Research on IP Address Access Control Method of Virtual Local Area Network

LI Jinfeng

(Changzhi Vocational and Technical College, Changzhi 046011, china)

**Abstract:** Aiming at the problem that the control method of virtual local area network (VLAN) is affected by the number of access users in the actual application, resulting in the control accuracy and time-consuming can not meet the expected requirements, the research on IP address access control method of virtual local area network is carried out. Through IP address location, user identification and IP address access control of local area network, an access control method for virtual local area network is proposed. Through comparative experiments, it is proved that the control method proposed in this paper can shorten the control time and promote the overall improvement of the operation efficiency of virtual local area network on the premise of effectively improving the accuracy of access control.

**Keywords:** virtual local area network; IP address; access control; user identification

### 0 引言

随着通信及互联网技术的快速发展, 互联网无论是速度, 还是规模都得到较大提升; 同时, 网络中的资源种类和数量不断增加, 相应的 IP 地址数量也不断增加<sup>[1-2]</sup>。在网络运行过程中, 经常性的网络调整和变动, 也使 IP 地址在管理上更加复杂。与互联网环境相比, 虚拟局域网中的 IP 地址数量尽管相对较少, 但仍然存在管理困难的问题<sup>[3]</sup>。在虚拟局域网中, 每台主机都需要局域网提供一个唯一的 IP 地址才能与

互联网连通; 同时, 为了确保虚拟局域网正常运行以及内部资源安全, 针对不同的 IP 地址访问进行控制具有十分重要的现实意义<sup>[4-5]</sup>。通过合理的访问控制可有效预防资源越权使用问题的产生。为此, 本文开展虚拟局域网 IP 地址访问控制方法研究, 进一步提高虚拟局域网的安全运行。

### 1 虚拟局域网 IP 地址访问控制方法

#### 1.1 局域网 IP 地址定位

为实现 IP 地址访问虚拟局域网的控制, 首先需

确定虚拟局域网中某台 IP 地址已知的设备所连接的交换机以及相应端口,达到对其定位的目的<sup>[6-7]</sup>。在定位过程中,可引入分析方法。虚拟局域网的网络结构示意图如图 1 所示。

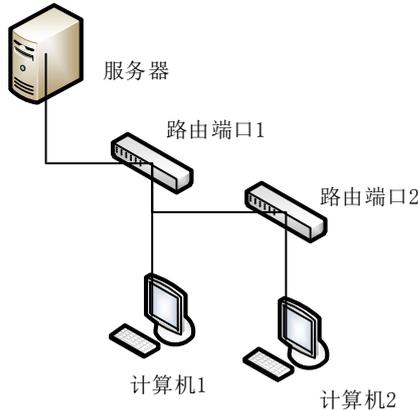


图 1 虚拟局域网的网络结构示意图

图 1 所示的虚拟局域网的网络结构由 1 台服务器、2 台交换机、2 台计算机组成。其中,2 台交换机分别对应 2 个路由端口,2 台计算机分别对应 2 个 PC 端口。利用分析方法,找出计算机与其直接连接的交换机端口,即可实现对局域网 IP 地址定位。在虚拟局域网中,找出 ARP 缓存列表,确定 IP 地址。由于 ARP 在实际应用中无法跨 VLAN 运行,因此选择 MSFC 作为连接方式。在局域网中,利用 VLAN 端口对 ARP 正确解释,并通过路由交换机完成指令的识别与执行<sup>[8-9]</sup>。完成指令输入后,在显示窗口中 IP 地址若能够与对应的 Router 设备相连接,即可实现交换机位置的定位和识别。如识别出交换机位置,则停止定位,直接将定位结果输出;如未识别出交换机位置,则需要重复上述步骤继续追查,直到找出不是交换机的定位结果,以此实现局域网 IP 地址的定位。

## 1.2 用户身份识别

局域网 IP 地址定位完成后,对访问虚拟局域网的用户身份进行识别。识别前,需对大量用户进行初次“海选”。将相似用户汇总到一个相似用户集中,在确保访问效率的基础上,将相似用户范围尽可能缩小。用户间相似性的量化利用公式(1)计算:

$$S(a,b) = \frac{|D(a) \cap D(b)|}{|D(a) \cup D(b)|} \quad (1)$$

式中:

$S(a,b)$ ——访问用户 a 与访问用户 b 之间的相似度;

$D(a)$ ——访问用户 a 在一定时间内经常访问 IP 地址的集合;

$D(b)$ ——访问用户 b 在一定时间内经常访问 IP 地址的集合。

通过公式(1)计算的  $S(a,b)$  在 0~1 之间。在识别过程中,为  $S(a,b)$  设定一个阈值  $k$ ,当  $S(a,b) > k$ ,说明用户 a 与用户 b 相似,可加入同一个相似用户集;当  $S(a,b)$  值  $\leq k$ ,说明用户 a 与用户 b 不相似,不能加入同一个相似用户集,以此完成用户的初步划分。

在此基础上,用户身份识别的具体步骤为:

第一步,在识别前,获取访问用户的真实基本信息和网络基本信息;

第二步,对能代表用户属性的身份信息进行格式化处理。通过公式(1)初步划分的相似用户集,仅代表用户访问 IP 地址行为的相似度。在身份识别过程中,不具备代表性,还需对用户身份与局域网中设定的用户身份访问类型共有属性相似度进行计算,计算公式为

$$Sim(B_t, B_v) = \left| \frac{P_v}{P_t} \right| \cdot Sim(P_t, P_v) \quad (2)$$

式中:

$P_v$ ——用户身份网络基本信息集合;

$P_t$ ——用户身份真实基本信息集合;

$B_v$ ——用户身份网络基本信息数据;

$B_t$ ——用户身份真实基本信息数据;

$Sim(P_t, P_v)$ ——用户身份共有属性平均相似度;

$Sim(B_t, B_v)$ ——用户身份访问类型与用户基本信息共有属性相似度。

根据公式(2)计算的  $Sim(B_t, B_v)$  取值范围为[0,1],其数值大小可以直接反映用户身份所属类型。

通常情况下,IP 地址访问用户数量越少,其个性

化程度越高,相应权重也越大。基于这一特点,将 IP 地址的权重定义为所有访问用户访问数的倒数。根据公式(1)和公式(2)的计算结果,进行倒序排列,并按照规定比例对前几名用户进行裁剪,得到最终用户身份认证集合。再从时间维度上对用户集进行裁剪,假设每一名访问用户的整体 IP 地址访问时间可用一个 24 维数据集合表示,利用余弦相似度计算方法,将所有访问用户的相似用户集访问时间相似度阈值进行设定。假设相似度阈值为  $m$ ,则将相似度  $\leq m$  的用户全部过滤,剩余用户即为完成身份识别的用户,以此内容,实现用户身份的识别。

### 1.3 IP 地址访问控制

实现用户身份识别后,对 IP 地址访问进行控制。首先,明确控制的 3 个要素为:主体(发出访问操作的用户)、客体(被访问的对象,如程序、进程、数据等)、授权策略(一套完整访问规则)。从数学角度对授权策略进行分析,将其看作一个矩阵,矩阵中的每一行看作一个主体,每一列看作一个客体,行与列的交点为访问节点。在控制过程中,引入网络分段和虚拟网络技术控制虚拟局域网用户完成访问,确保用户能够在局域网中合法获取所需资源,同时又能够限制其他用户对该用户私有资源的访问,以此提高局域网访问的安全性。

在实际应用中,确定主体用户身份信息后,针对主体用户整个访问过程继续进行控制。访问控制包含用户身份认证、用户授权控制 2 方面。其中,用户授权控制可看作是对主体和客体的控制。根据不同的授权策略,共包含 4 种类型的集中控制方式:第一种,自主访问类型;第二种,强制访问类型;第三种,基于角色的访问类型;第四种,基于任务的访问类型。针对 IP 地址访问的有效控制可促进用户信息完整性和机密性的提升。在控制过程中,还需要对授权颁发是否影响网络可用性指令,是否能够获取拒绝服务攻击信息等进行判断。

## 2 仿真实验设计

为进一步验证 IP 地址访问控制方法的实际应用

效果,选择传统基于路由器访问控制列表的控制方法作为对照组,将其应用时的参数设定作为对照条件,本文控制方法作为实验组,开展对比实验。

实验在某校园虚拟局域网环境进行,选择控制准确率以及控制耗时为评价指标,对两组控制方法进行综合评价。该校园虚拟局域网包含教师身份访问、学生身份访问、校内身份访问(除教师和学生身份以外的用户,如学校管理员、辅导员等)、校外身份访问 4 种访问类型。4 种访问类型对应 4 个访问通道,随机选择 1 000 名实验志愿者作为访问用户,根据 4 种访问类型进行随机划分,在不知道具体划分情况的前提下,利用两组访问控制方法对其进行控制,对比其访问结果。

### 2.1 控制准确率比较

为实现实验组和对照组控制准确率的对比,按公式(3)对控制结果参数进行计算:

$$\gamma = [(x_1 + x_2 + x_3 + x_4) / n] \times 100\% \quad (3)$$

式中:

$\gamma$  ——控制结果的准确率;

$x_1$  ——正确控制教师身份用户访问数量;

$x_2$  ——正确控制学生身份用户访问数量;

$x_3$  ——正确控制校内身份用户访问数量;

$x_4$  ——正确控制校外身份用户访问数量;

$n$  ——访问校园虚拟局域网的总人数,在本文实验中, $n$  的最大取值为 1 000。

根据公式(3),计算实验组和对照组 2 种控制方法的准确率,实验结果如表 1 所示。

表 1 实验组与对照组控制方法准确率结果对比表

用户访问数量/名	实验组控制准确率/%	对照组控制准确率/%
200	98.32	69.23
400	97.36	68.13
600	99.23	59.23
800	95.31	58.23
1 000	97.16	54.21

由表 1 可以看出, 实验组的控制准确率均超过 95.00%; 而对照组最高控制准确率 69.23% 出现在用户访问数量为 200 名时, 并且随着用户访问数量增加, 对照组控制准确率呈现明显下降趋势。由此可知, 实验组控制方法的准确率更高, 且不受用户访问数量的影响。

## 2.2 控制耗时比较

以上述实验内容为基础, 对 2 种控制方法的 IP 地址访问控制耗时进行对比<sup>[10]</sup>。从 IP 地址访问开始, 到本文控制方法为其自动分配访问通道实现访问为止的时间为控制耗时, 2 种控制方法的耗时记录如图 2 所示。

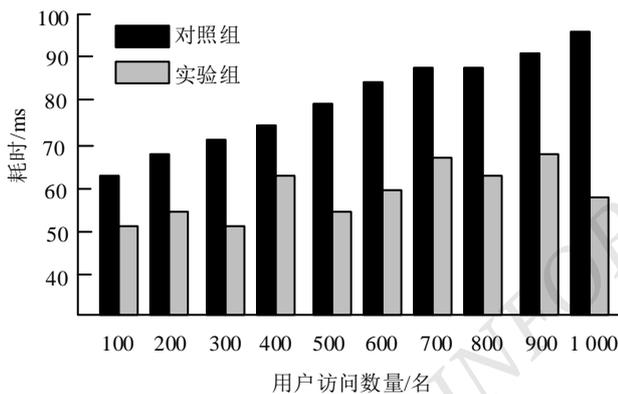


图 2 实验组与对照组控制耗时比较图

由图 2 可以看出, 实验组的控制耗时最高为 68.32 ms, 对照组的控制耗时最高为 98.32 ms; 在用户访问数量相同的情况下, 实验组的控制耗时均小于对照组。因此, 通过实验进一步证明, 实验组的控制方法控制耗时更短, 控制效率更高。

综合上述 2 组实验结果得出, 本文提出的控制方法在真实虚拟局域网运行环境中, 在保证控制准确率

的前提下, 可提高控制效率。

## 3 结论

本文提出一种面向虚拟局域网的访问控制方法, 并通过对比实验, 从控制准确率和控制耗时 2 方面验证了本文控制方法的可行性和优势。在今后的研究中, 还将充分利用虚拟局域网中交换机在定位网络设备中的应用优势, 开展更加深入的访问控制研究; 利用其实现对网络故障的快速排查, 进一步提高虚拟局域网运行环境安全性。

## 参考文献

- [1] 王贵. 路由器访问控制列表在计算机局域网网络安全中的应用[J]. 电子世界, 2021(19):174-175.
- [2] 李倩. 网络安全多层面联动主动防御体系的研究与应用[J]. 自动化与信息工程, 2019, 40(4):20-24.
- [3] 尹虹, 田涛. 基于无证书公钥密码的铁路通信网访问控制方案研究[J]. 铁路计算机应用, 2020, 29(8):48-51.
- [4] 古丽色曼尔·艾尼瓦尔. 浅谈办公局域网中心控制机房设备管理与维护[J]. 电脑知识与技术, 2020, 16(17):54-55.
- [5] 余爱民, 赖声礼, 陈荷, 等. 无线局域网信息安全主流技术的探讨[J]. 机电工程技术, 2003, 32(5):18-19, 22.
- [6] 王焱, 夏长春, 匡兴红. 水下机器人的设计与 CSMA/CD 局域网控制系统研究[J]. 制造业自动化, 2021, 43(8):22-28, 51.
- [7] 刁海平. 考虑需求响应的电力负荷自动调度方法[J]. 自动化应用, 2021(11):111-112.
- [8] 牛玉坤, 魏凌波, 张驰, 等. 基于比特币区块链的公共无线局域网接入控制隐私保护研究[J]. 网络与信息安全学报, 2020, 6(2):56-66.
- [9] 梁雪青, 杜舒明, 刘超, 等. 基于数据挖掘的电力数据调度传输方法[J]. 数字技术与应用, 2021, 39(12):77-79.
- [10] 高静晗. 基于 AutoCAD 的室内建筑装饰布局设计研究[J]. 信息与电脑(理论版), 2021, 33(12):35-37.

## 作者简介:

李晋峰, 男, 1974 年生, 本科, 讲师, 主要研究方向: 计算机网络应用。E-mail: pu57797193@126.com