IP 设备可信接入控制技术①

葛晓滨[1]，许 剑[2]

[1](安徽财贸职业学院 雪岩贸易学院，合肥 230601)
[2](合肥恒卓科技有限公司，合肥 230022)

摘 要：提出了 IP 设备可信接入控制技术。通过该技术的应用，实现了大中型企业信息网络中所有 IP 设备的接入行为的管理与控制，系统采用基于 Linux 系统的 Python 语言进行开发，用户在 Web 管理端通过可视化的界面进行 IP 资源的规划、分配，同时可以制定各种 IP 使用策略。系统实现了对信息网所有 IP 设备接入行为的可控、在控，从而提高了信息网络的安全性。

关键词：IP 设备；可信接入；控制技术

Technology for Trusted IP Access Control Equipment

GE Xiao-Bin[1], XU Jian[2]

[1](Xueyan Trade College, Anhui Finance and Trade Vocational College, Hefei 230601, China)
[2](Hefei Heng Zhuo Technology Co., Ltd., Hefei 230601, China)

Abstract: Trusted IP equipment proposed access control technology is proposed in this paper. The adoption of this technology can achieve a medium-sized enterprise information network for all IP devices in the management and control of access behavior. The system based on Linux system Python language to develop and management of end users in the Web interface through the IP visual resource planning, allocation, and can be used to develop a variety of IP strategy. The system realizes the information network for all IP devices on the access behavior of the control, in control, thus enhancing the security of information networks.

Keywords: IP device; reliable access; control

随着企业信息网络规模的增长，网络设备和网络拓扑结构的日益复杂，如何有效地管理整个网络系统中的 IP 地址，解决地址过多和进行有效的分配 IP 地址成为困扰很多企业的问题。如果没有有效的管理，可能导致网络可用性和服务质量的下降，甚至网络的崩溃，还可能造成大量商业损失。

为此我们研发了 IP 设备可信接入控制与管理系统。该系统提高了 IP 地址使用率，实施了对网络的 IP 地址使用的有效管理，并能对常见的 IP 地址故障进行自动化处理。通过该系统实现了信息网入网和运行的可控性，提高信息网络的安全性。

1 系统功能及原理

1.1 系统主要解决的问题

对入网设备进行有效管理和保证网络安全的问题日益突出。参考文献[1-5]对此均有一定的探讨，总结网络设备接入主要存在的问题有：

(1) 用户终端能够随意设置 IP，造成网络 IP 地址冲突，甚至与关键应用服务器地址冲突。

(2) 很多未经授权的计算机没有经过接入流程审批，任何终端只要接入到网络中就能够访问业务系统或其他终端 。

(3) 对于网络设备的随意接入(例如无线 AP)、终

① 基金项目:安徽省高等学校省级自然科学研究项目
收稿时间:2010-08-19;收到修改稿时间:2010-10-03

端设备的转移变更没有有效的技术手段能够发现和阻止。

(4) 缺少集中网络资源整体规划,无法掌握网络资源使用状况，IP 资源浪费情况严重。

(5) DNS 域名解析较为混乱，应用采用 IP 地址直接访问，难以记忆和管理，无法解析到重要网络设备域名，缺少统一 DNS 整合工具。

1.2 系统功能

IP 设备可信接入控制与管理系统适应于信息网络中所有 IP 设备的接入行为的管理与控制。系统功能主要有信息监控、IP 资源管理、DHCP 管理、DNS 管理、交换机管理、报表管理、系统管理等。系统分为后台服务程序和 WEB 管理端两部分，用户在 WEB 管理端通过可视化的界面进行 IP 资源的规划、分配，同时可以制定各种 IP 使用策略，包括：时间、新设备接入、白名单、IP-MAC 绑定、分组管理等。后台服务程序根据用户配置的 IP 信息，对网络中的接入行为进行监测与控制。本系统实现了对信息网所有 IP 设备接入行为的可控、在控，从而提高了信息网络的安全性。

系统的后台服务程序是基于 Linux 平台采用 Python 语言进行开发，用以保证系统的稳定性与多平台的可移植性。系统以标准 Web Services 方式向外提供各种操作、查询、控制接口，保证良好的可集成性和扩展性，方便系统和信息网络其他管理产品集成，满足全面管理、团队协作、信息综合、业务协同、流程连贯的整体需要。

1.3 实现原理

IP 可信接入根据预先的设定控制终端用户的访问权限，检查用户的身份及终端信息，有效阻止不符合身份认证的设备接入及访问网络，使得在未通过认证的情况下，用户不能获得访问中心应用系统的权限。

实行 IP 地址管理最基本的方法是实施 IP－MAC 绑定措施,传统 IP－MAC 地址绑定策略需要手工操作交换机，使用交换机专有的命令，专业性太强，对大量网络设备进行 IP－MAC 维护工作时工作量太大,实施起来困难，而且容易出现差错，造成网络运行故障。通过使用 IP 可信接入，我们可以使得管理员可以方便的对用户 IP 地址进行分配、管理和定位，有效避免多个管理员之间分配 IP 资源的冲突，同时避免对大量的网络设备进行 IP－MAC 绑定信息的维护,并保证所有相关设备和系统中的数据一致性，减少了网络管理人员在 IP 分配和管理上的人力投入，使得网管人员在处理网络事件时可以通过资料检索快速定位到具体用户和设备，减少事件判断和定位的时间。系统的主界面如图 1 所示。

图 1　系统主界面

2　系统关键技术

在 IP 设备可信接入控制与管理系统的设计实现上，我们采用如下的关键技术：

2.1 抽象并建立交换机模型，兼容不同交换机

针对网络中可能出现的不同厂商、不同型号交换机的状况，我们分析需要的操作命令子集，抽象出交换机控制模型，并针对不同交换机建立相应的命令模型。利用该模型程序能够统一操作不同型号的交换机，做到兼容不同厂商、不同型号的交换机，同时方便系统扩充更多型号的交换机。

同时针对各地交换机管理需要，交换机操作方式上兼容 Telnet 和 SSH 两种管理方式，使用仿真程序完成对交换机的操作。

2.2 动态扫描与静态绑定管理模式组合策略

动态扫描模式是采用轮询交换机的方式，动态化地从接入层交换机获取当前接入的设备信息，并且和合法设备进行比对，找出未被授权接入网络的设备，并根据系统策略判定是否应当阻止，对于需要阻止接入的未授权设备，直接在接入层交换机上阻断接入行为。此模式适合于规模较小的网络，同时在阻止策略上具有很高的灵活性，可以适应各种管理需求。

静态绑定模式是直接将合法授权的 IP 信息写入三层交换机，同时进行指定端口绑定，只有已授权 IP 才可通过，从而达到阻止非法接入 IP。此模式适合于大规模网络，同时系统负载小、实时性高。

两种模式可根据用户需要灵活配置组合。

2.3 设备、交换机、IP 绑定技术

根据设备实际使用情况和使用人员，采用人工指定各个设备可以接入的交换机及端口，并指定设备可以使用的 IP 地址，实现设备、IP 和交换机绑定，防止未被授权接入的设备接入和设备在不同地点迁移。

利用设备和交换机的绑定关系，完全避免未经授权的设备访问网络。

2.4 IP 资源利用情况可视化分析技术

根据现有 IP 资源情况和 IP 地址利用情况，动态分析不同地点、不同子网、不同楼宇、不同部门、不同 VLAN 的 IP 资源使用情况，给 IP 资源调整和网络结构调整提供决策依据，并且通过图表直观呈现，具有可视化分析特点。如图 2 所示。

图 2 IP 资源信息监控

在企业端通过集中式网络规划管理，可以及时发现网络资源使用紧张的地址段，通过逐级委托的管理方式可以将 B 类地址分配给需要使用的网络分支。

2.5 结合 DHCP 功能实现合法 IP 地址分配

将申请过程中收集到的 MAC 地址信息和分配的 IP 地址信息写入 DHCP 配置文件，由 DHCP 来管理整个局域网内网络分配情况，这样可以容易保持终端用户信息的正确和完整，通过 DHCP 分配和 IP－MAC 绑定的方式向终端用户提供固定的 IP 地址，做到和现有手工分配静态 IP 方式兼容。

2.6 核心服务技术平台的开发

在网络环境下，系统应具备 24*7 运行能力，为了保证系统的稳定性，核心服务采用 Linux 系统平台构建。我们采用开源语言 Python 进行开发，它对操作系统平台没有依赖性， 而且 Python 语言写的程序不需要编译成二进制代码。

系统的表现层基于.NET 平台体系构建。.NET 开发平台是一组用于建立 Web 服务器应用程序和 Windows 桌面应用程序的软件组件。.NET 开发平台是一组用于建立 Web 服务器应用程序和 Windows 桌面应用程序的软件组件，用该平台创建的应用程序在 Common Language Runtime（CLR，通用语言运行环境）的控制下运行。采用.NET 来进行系统开发更易于重用别人创建的代码组件的程序设计模型，通过向开发者提供已有的组件，消除了重写底层例程的必要，从而提高开发者的开发效率。同时选用 C#开发语言，可以消除或减少其他开发语言的易出错结构的使用，以及使用强迫对所有代码组件间的交互点作清晰定义的编程模型，增强了软件的可靠性。

3 技术创新点

IP 可信接入控制统一管理所有接入企业网络的 IP 资源，提高了整个信息网运行可靠性。应用 IP 可信接入控制后，我们可以对数量众多的终端实现安全、有效的准入控制。从技术手段上确保了接入网络设备的审批流程，保障了网络应用系统的安全。我们采用以下的技术创新点实现系统功能：

3.1 集中式网络管理、逐级委托管理方式

大中型网络 IP 地址分配，一般是由总部统一规划、分配，再由各分支机构详细划分网段并分配到部门、个人、设备。在管理上，总部管理整体 IP 地址规划并管理总部本部 IP 地址分配，分支机构分配到的 IP 地址由他们自行管理或者做进一步划分，按照网段逐级委托管理。

3.2 能够管理和控制多种网络设备

支持多种网络设备管理，能够管理和控制各类 Cisco、华为、华为 3COM、北电、Foundry 等网络设备；使得管理员可以避免对大量的网络设备进行 IP－MAC 绑定信息的维护，保证所有相关设备和系统中的数据一致性。

3.3 动态扫描与静态绑定的两种交换机控制管理模式

在三层交换机上采用静态绑定方式接管，在二层交换机上采用动态扫描方式接管，双管齐下的控制方式保证 IP 地址的合法性，以及网络使用的规范性。

3.4 便捷的 DNS 域名管理

分布式部署 DNS，并根据分支机构情况完成和 Windows 活动目录（域控制器）、DNS 整合，实现公用域名集中解析，各分支机构子域名分布式解析；实现各分支机构自己注册域名、域控制器临时域名、群

集临时域名的解析；包括和域控制器集成提供反向注册和解析；并能够进一步规范了服务器、网络设备、桌面终端命名。

3.5 提供二次开发的标准接口

提供二次开发的标准接口（Web Service 接口），能够与现有管理系统整合（例如信息网管理系统、桌面管理系统），形成统一管控工具。

4 系统成效

IP 可信接入控制系统在网络管理上可以协助我们可以获取如下的应用上的收益：

(1) 实现 IP 可信接入，提供有效的 IP 资源的使用和管理管理工具和统计工具，在 IP 地址资源利用情况分析的基础上，我们可以更合理分配和使用 IP 地址资源。

(2) 降低信息网络管理成本。提高分配 IP 地址的效率，并且通过 IP 地址可以直接追踪到终端用户，这使得网络管理人员制定各项网络管理策略将会更直接、更有效，并使得网络管理人员在查找、分析信息网络故障时大大缩短查找和定位所需要的时间。

(3) 可以对网络安全事件责任到人。在 IP 可信接入中 IP 地址和终端用户是一一对应的，这样可以确保网络中的 IP 是由经过授权的用户产生的，通过由 IDS、防火墙等网络安全设备记录下来的用户访问日志中的 IP 地址信息即可定位到具体责任人，也可以从一定程度上避免信息安全事件的发生。

5 结束语

IP 设备可信接入系统对信息网络的 IP 接入行为进行有效的可控、在控管理。整个系统具有很强的扩展性和可移植性。系统使 IP 地址资料信息管理规范有序，对数量众多的网络设备和终端实现了安全、有效的准入控制，减少了网络管理和运行成本，达到推行入网准许控制、IP 管理自动化的目标。经应用实践证明，本系统是一种先进的、有效的信息网络 IP 授权控制管理工具。

参考文献

1 王海涛.新一代宽带 IP 网络综合接入设备的设计探讨.电视技术,2004,(3):35–37.

2 段惟荣.MMDS 宽带固定无线接入技术综述.无线电工程,2003,33(1):35–38.

3 Al Chisholm. A Technical Overview of the OPC Dada Access Interface. Intellution Inc. 1999: 78–81.

4 郑志蓉.可信接入系统.网络安全技术与应用,2008,(9):32–33.

5 秦超.基于数字证书认证的电力安全拨号认证系统.电力系统自动化,2009,(10):52–55.

（上接第 226 页）

态环境中 PDIGA 算法与其他基于移民策略的遗传算法相比，具有最快速的适应新的环境，追踪最优解的能力，表现出了很好的性能，能够较好的适应环境的动态变化。

参考文献

1 Cobb HG., Grefenstette JJ. Genetic algorithms for tracking changing environments. Proc. of International Genetic Algorithms Conference, 1993.

2 Grefenstette JJ. Genetic algorithms for changing environments. IEEE Proc. of Congress on Evolutionary Computation, 2004: 1278–285.

3 Cheng H, Yang SX. Genetic algorithms with elitism-based immigrants for dynamic shortest path problem in mobile Ad Hoc networks. IEEE Congress on Evolutionary Computation (CEC 2009), 2009: 3135–3140.

4 Yang S. The primal-dual genetic algorithm. Proc. of the 3rd International Conference on Hybrid Intelligent System, 2003.