国内大型企业终端管理技术探索与解决方案研究

陆良伟，岳峙君，袁 懿
（迈普通信技术股份有限公司，四川 成都 610094）

摘 要： 随着网络的高速发展与网络数字化的转型，接入网络中的终端数量呈爆炸式增长，如何进行智能、安全的管理终端就显得尤为重要。结合企业的终端管理现状，从安全隐患、终端接入风险管控等角度出发，设计了通过自动学习终端特征从而智能识别终端类型的方法，并通过完善的终端准入功能，实现了终端智能识别与安全准入网络的终端管理系统，从而保障企业网络安全。

关键词： 自动学习；智能识别；方案设计；网络安全
中图分类号： TN918 **文献标识码：** A DOI：10.16157/j.issn.0258-7998.212279

中文引用格式： 陆良伟，岳峙君，袁懿. 国内大型企业终端管理技术探索与解决方案研究[J].电子技术应用，2021，47(12)：39-43.
英文引用格式： Lu Liangwei，Yue Zhijun，Yuan Yi. Research on the exploration and solution of terminal management technology for large domestic enterprises[J]. Application of Electronic Technique，2021，47(12)：39-43.

Research on the exploration and solution of terminal management technology for large domestic enterprises

Lu Liangwei，Yue Zhijun，Yuan Yi
（Maipu Communication Technology Co.，Ltd.，Chengdu 610094，China）

Abstract： With the rapid development of the network and the transformation of network digitization，the number of terminals in the access network is explosively growing，how to carry out intelligent，safe management terminal is particularly important. Combined with the current situation of enterprise terminal management，from the perspective of security risks and terminal access risk control，the paper designs a method of intelligent identification of terminal types through automatic learning terminal characteristics，and realizes terminal intelligent identification and secure access network terminal management system through perfect terminal access function，so as to ensure enterprise network security.

Key words： automatic learning；intelligent recognition；scheme design；network security

0 引言

2020年是信息技术应用创新产业全面推广的起点，发展自主创新的信息技术应用、创新产业生态是网络经济数字化转型，提升产业链发展的关键，也是国家的重要发展战略。同时，在政府、银行等体系中，对于接入网络中的终端进行规范管理和接入安全管控有更高的要求，是保障企业网络安全的重要手段。

随着网络的高速发展和网络数字化的转型，接入网络中的终端的数量和终端类型都在飞速增长，数字化终端的广泛应用也带来了一系列的管理问题和安全问题[1]。网络安全是国家网络安全的重要组成部分，网络安全等级保护2.0[2]也体现了国家对于网络安全的政策性要求。

根据调研，目前许多政府机构和企业对于接入网络中的终端仍采用人工登记管理，由管理员统一进行终端资产维护。随着大量新型数字化终端的增加，人工维护成本和维护难度也在同步上升；同时对于接入网络中的终端类型变化、位置变化等，管理员无法实时感知，从而对终端私接、未经授权接入网络、入侵攻击等一系列的安全隐患无法及时干预处理，存在很大的安全隐患。在传统的终端识别方案中，当终端类型发生变化时，需要人工介入进行更新升级，无法智能解决终端识别问题，进一步增加了维护成本和管理难度。

本文通过设计与实现智能终端管理解决方案，解决政府和企业管理网络中海量终端管理难的问题，在节省人力成本、提升管理效率的同时，实现终端智能识别、仿冒检测、接入位置变化感知，保证准入网络的中的终端安全，对政府和企业的网络安全保护具有重要意义。

1 终端管理系统现状概述

目前多数的政企单位在网络安全建设过程中，由于

受条件和其他因素的限制，导致现在的终端管理系统比较落后，在当前全球网络安全形式严峻、网络攻击层出不穷的现状下，政企网络安全面临着巨大的风险和挑战。根据对现有终端管理系统的调研，发现多数终端管理系统普遍存在不足。

现有的终端安全管理系统多是孤立的针对某一个方面的安全防护，安全防护体系彼此孤立，无论从系统层面还是从数据层面都无法进行有效整合，从而无法应对目前大数据时代新型的网络安全威胁[3]。

目前部分终端管理系统，其安全防护方面通常与厂商自身的硬件配套，而这些硬件设施通常比较昂贵[4]，对于企业来说使用成本很高，而且面临着对现有网络的组网进行修改的风险，如 360 网神终端安全管理系统，其终端安全检测功能就依赖于它的硬件 NAC 设备，而这些设备通常是很昂贵的。

企业内部网络包含着多种多样的网络设备和终端设备，现有的管理通常依赖于安保部门进行终端接入管控，但是在复杂的应用环境中，这不仅增加了人工管理成本，还无法保证终端私接的情况发生，一旦发生入侵，系统无法及时感知，对企业的网络安全系统造成极大的安全隐患[5]。

为方便企业进行终端资产管理，需要终端管理系统具有对终端类型的识别功能，而现有的系统在终端类型识别上并不智能，通常需要用户介入，进行更正或者自定义一些规则，如奇安信的终端管理系统在对一般类型的终端(除摄像头等)进行识别时，存在需要用户建立匹配特征的情况，才能对终端类型进行识别。也有系统通过其提取终端特征，建立特征库进行识别[6]，但是在系统无法识别成功时，就需要专业人员介入，进行终端特征的维护和升级，无法实现终端类型智能识别和升级。

综上所述，现有的终端管理系统在准入控制，安全防护以及智能识别终端类型等方面还存在这一定的不足。针对这些不足，本文提出了一种智能终端管理解决方案的设计与实现，并通过实践，有效地解决了企业在终端管理中面临的问题。

2 方案架构

本方案基于终端管理系统现状，采用了一种模块化、可扩展、可升级、支持多协议的控制器框架，主要包括开放的北向 API、控制平面，以及南向接口和协议插件。其中控制平面包含一系列的功能模块，可动态组合提供不通过的服务。南向链接多种协议插件，并且屏蔽了不同协议之间的差异，方案架构如图 1 所示。

图 1 所示的架构中，大致可以分为三层结构：业务服务层、控制平台层以及物理和虚拟网络设备层，通过北向接口和南向接口将三者连接。

业务服务层主要为网络应用服务，处理网络事件，从而对网络进行控制和引导。通过这一层的功能实现，用户可以根据实际需求从控制界面对下层模块进行调用，通过配置规则，实现控制与转发分离，以实现对网络的

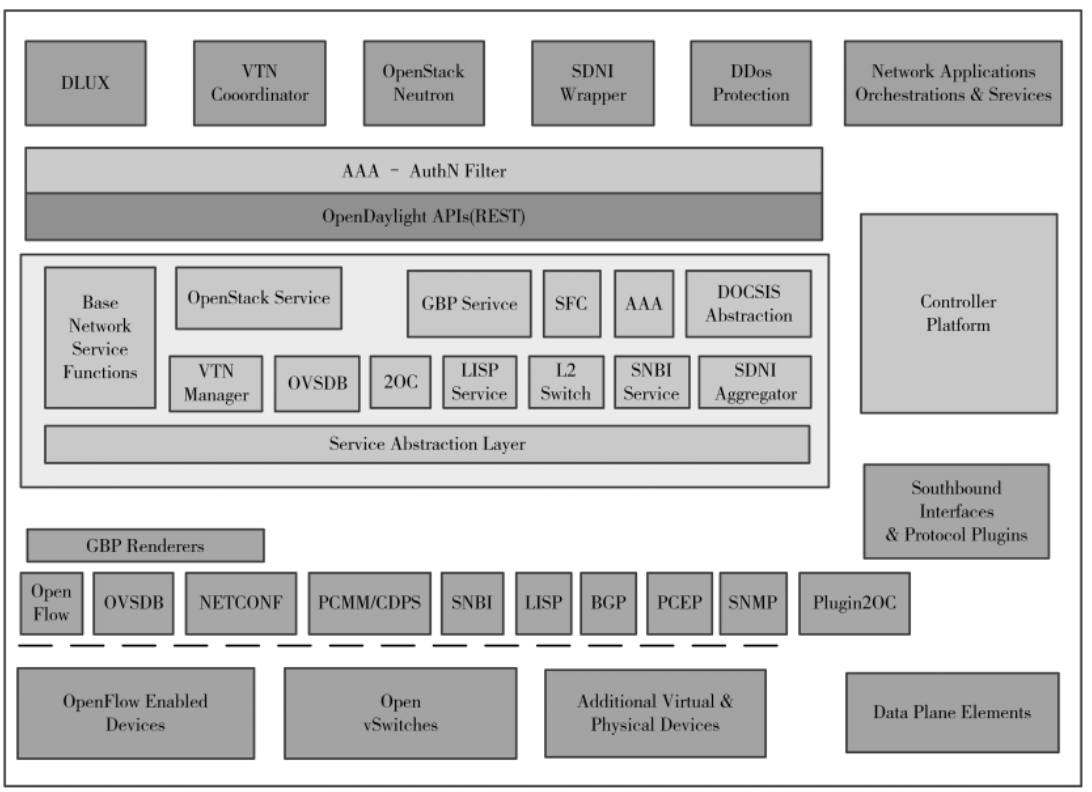

图 1 智能终端管理方案架构示意图

管控，大大提高了网络管理的灵活性。

控制平台层包括基本的控制器服务功能模块，主要包含网络发现、拓扑管理、配置下发、统计管理等。通过将网络中的网络设备发现到控制平台，统一进行拓扑呈现和网络设备管理，控制平台层接收业务服务层的请求，将业务动作通过配置下发模块，将业务配置下发到与南向接口关联的网络设备上，实现对网络的控制。

物理和虚拟网络层主要由物理设备和虚拟设备组成，例如交换机、路由器等在网络短点间建立连接，构成用户的网络。用户的各类终端均通过边缘接入设备连接到这个网络中，以实现用户网络和业务的构建。

3 关键技术创新设计

3.1 基于自动学习终端特征的终端类型识别技术设计

3.1.1 终端特征自动学习流程

针对终端在不同工作模式下，其特征信息不一样，从而导致 SDN 控制器无法准确识别终端类型的问题，设计了基于自动学习终端特征的终端类型识别方法，通过设置开放期，在开放期内定时收集终端特征并进行特征匹配和自动学习，自动升级终端识别指纹库，无需人为介入即可完成终端识别指纹库的升级，保证终端类型的准确识别，终端自动学习模型如图 2 所示。

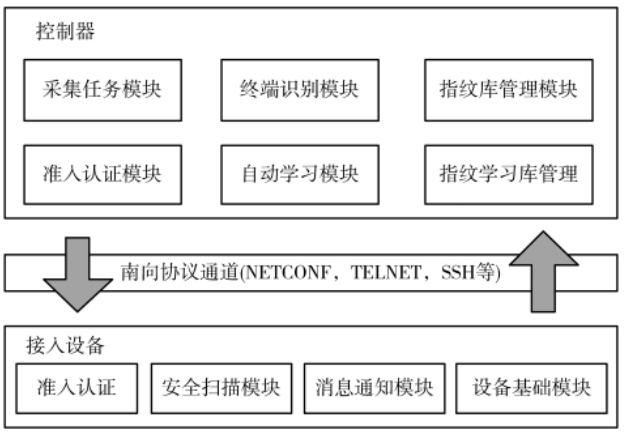

图 2 终端特征自动学习模型图

图 2 的终端特征自动学习模型主要包含了控制器和接入设备两个部分。其中，设备主要通过安全扫描模块对从设备接入的终端进行安全扫描，采集终端信息；控制器则主要是通过采集任务模块，当终端准入认证通过后，或者开放期定时采集，向设备下发扫描任务进行终端信息收集。根据采集到的终端信息，再提取成终端特征，对终端进行类型识别。

根据上述自动学习模块，终端特征自动学习主要流程如图 3 所示。

图 3 所示的终端特征自动学习流程中，通过自动学习终端指纹特征自动升级指纹库，以实现对终端的智能识别，其主要流程包括如下几个步骤：

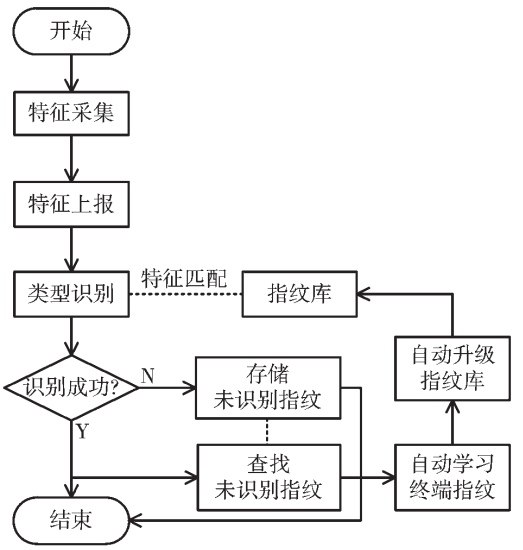

图 3 终端特征自动学习流程图

(1)采集特征：触发控制器进行特征采集有两种方式：一是终端从边缘设备接入网络，通过准入认证模块认证通过后，控制器会对终端接入的设备下发采集任务，采集终端的信息；二是通过配置开放学习期，在开放学习期内控制器会主动定时去采集所有接入网络的终端信息。

(2)特征上报：设备采集到终端信息后，会通过南向通道向控制器上报终端信息，供控制器进行特征提取和识别。

(3)类型识别：控制器收到设备采集到的终端信息后，会根据终端信息提取终端的特征，提取完成后，将提取的特征与指纹库进行匹配，匹配成功则识别成功，否则匹配失败。

(4)未识别指纹存储：针对终端未匹配指纹库成功的情况，会将当前未匹配成功的终端特征进行存储，用于后续进行终端特征学习。

(5)自动学习特征：当终端某一次的扫描特征匹配指纹库成功，即识别成功后，此时会进入自动学习流程。首先会从指纹学习库中查询该终端是否存在待学习的终端特征，如果有，则将这些特征逐一学习成本次成功识别的终端类型(如果有 n 条待学习的特征，就会学习为 n 条新的终端特征)，并将这些学习过后的终端指纹特征自动升级到指纹库。当下一次扫描到终端信息，只要终端信息之前学习过，那都可以成功识别出该终端的类型。

3.1.2 终端特征自动学习算法

终端特征的自动学习算法依赖于终端特征信息的收集和提取，系统将提取到的终端特征组与特征库中的终端指纹进行匹配，根据匹配结果最终得到终端的识别结果。当终端特征与指纹库匹配失败，即终端类型识别失败时，系统就会对该终端的特征进行记录，并标记该

终端为开始自动学习的状态，开始为该终端建立自动学习单元。自动学习算法过程如图 4 所示。

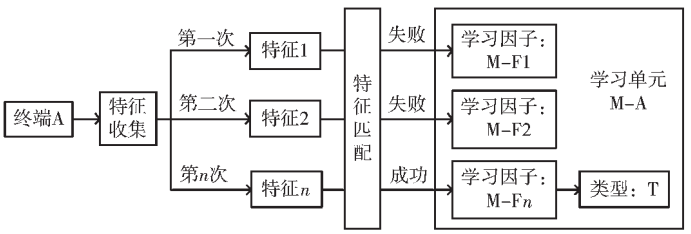

图 4 自动学习算法

如图 4 所示，终端 A 具有 n 种工作模式，在每一种工作模式下，控制器收集到的终端特征都不相同，分别为特征 1、特征 2、特征 n。当特征 1 第一次被收集到后，系统对该终端进行指纹库特征匹配，匹配结果为失败，此时系统就会为终端 1 建立学习单元 M-A，M 代表终端的 mac 地址唯一标识，表示由终端 A 建立的学习单元。

终端 A 前 $n-1$ 次均匹配特征库失败，在学习单元中根据每次收集到的不同特征，建立起该终端的学习因子 M-F1、M-F2 一直到 M-Fn-1，直到第 n 次收集到的终端特征匹配成功，根据特征因子 M-Fn 识别出了终端类型 T（其中 F1、F2、Fn 代表终端的不同特征信息），此时自动学习单元就会将之前的 $n-1$ 个学习因子逐一与类型 T 进行配对，并将配对后的对应终端特征录入终端特征指纹库，自动升级丰富特征库。

当终端第 $n+k$ 次收集到的特征进行指纹库特征匹配时（k 为第 n 次之后的任意一次），仍然匹配失败，由于之前第 n 次的时候该终端已经成功识别了类型为 T，则直接将类型 T 与本次收集到的特征进行配对并加入指纹库即完成特征自动学习。

3.2 终端安全管控技术设计

为实现感知系统中的终端类型变化、接入位置变化，使客户可以第一时间发现系统中的异常终端，并进行及时处理，对终端进行安全管控设计。当系统中出现终端位置变化、类型变化等，可以通过告警提示或者提前配置的策略对终端进行管控，防止系统出现安全隐患，终端安全管控流程如图 5 所示。

基于图 5 的安全管控流程，当终端接入系统后，其位置信息和类型特征等发生变化，终端管理系统可以及时感知到终端的信息变化，为用户进行告警或阻断终端等，从而达到保护网络，防止恶意入侵、终端仿冒等安全问题。终端安全管控流程主要步骤如下：

(1)终端接入网络后，需要进行准入认证，认证通过后会首先将该终端与基线终端信息进行对比，如果发现接入位置发生了变化，则会进行相应的告警或者根据用户事先配置的策略进行阻断。

(2)当在步骤(1)中终端未被阻断时，会继续对该认证通过的终端进行识别，对终端类型识别完成后，再进行后续处理。

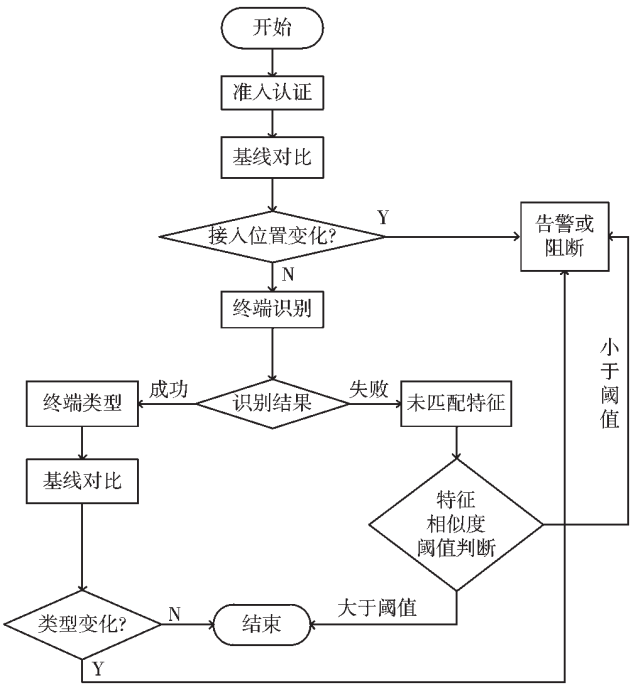

图 5 终端安全管控流程图

(3)如果本次对该终端识别成功，则会与基线终端进行判断，如果基线终端的类型与本次识别的类型不一致，则认为该终端是仿冒终端，发生了安全事件，此时就会进行告警通知或者阻断处理。如果发现该终端此时还没有基线，则会将本次识别结果以及终端认证上线携带的位置信息作为基线终端信息。

(4)如果本次对终端识别失败，此时则会根据用户预先设置的阈值进行特征相似度比较，当相似度大于阈值，则认为没有发生仿冒，不进行告警或阻断；如果相似度小于阈值，则认为终端发生了仿冒，此时会作为安全事件进行告警或阻断处理。

根据上述流程，保证终端在接入网络后，其信息变化能及时被系统感知并通知用户，便于用户及时处理网络中的异常终端信息，避免恶意入侵网络。通过相似度阈值判断，也可以避免系统在识别失败时出现误报仿冒，影响用户判断，从而灵活控制网络中的终端。

4 应用与实践结果分析

4.1 应用场景分析

智能终端管理解决方案的主要应用场景是典型的三层组网或扁平化二层组网结构的大楼或园区，同时支持通过广域网连接主园区的扁平化二层网络，边缘网络设备是交换机或者是交换路由一体机，其应场景如图 6 所示。

图 6 是智能终端管理解决方案的主要应用场景，终

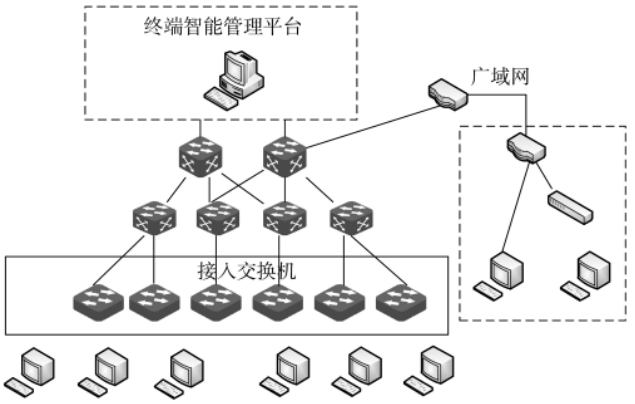

图 6 智能终端管理解决方案应用场景图

端通过边缘接入设备接入到网络中，由智能终端管理平台对入网终端进行统一的准入认证管控、资产维护、安全防护和预警等。根据对终端多特征自动学习，自动升级特征库，从而智能识别终端类型，进入资产维护和安全管控，对全网终端进行智能管理，保障网络安全。

4.2 实践结果分析

通过在客户环境中进行应用与实践，智能终端管理解决方案有效地解决了客户面临的终端管理困难、终端资产难以维护、网络面临安全风险等问题，对于海量终端管理和维护、保障网络安全具有重要意义。

智能终端管理解决方案通过设计自动学习终端特征，有效解决了终端在不同工作模式下特征不同而导致识别不准确或识别错误的问题。整个过程无需人为介入，系统便可自动学习终端特征并升级终端指纹库。对于识别成功的终端，用户可以在系统中进行资产维护和管理，而不需要人为对网络中的终端进行统计，大大节约了人力成本和维护成本。在客户环境中进行实践，加入特征自动学习前后的识别成功率对比如表 1 所示。

表 1 自动学习前后识别成功率对比表

	终端数量	识别成功数	识别成功率/%
自动学习前	50 000	12 893	25.78
自动学习后	50 000	48 624	97.24

通过表 1 可知，加入终端特征自动学习后，系统对终端类型的识别成功率有了明显的提升。

根据终端智能识别功能，设计终端安全管控，有效地解决了终端位置变化、终端仿冒、私接等用户感知不及时的问题，通过告警和配置策略进行阻断，使用户可以快速发现网络中的异常终端从而进行相应的管控处理，达到了保障网络安全的目的。

5 结论

通过一体化的终端管理平台，实现对等级保护等合规要求中的准入控制、资源控制、资产管理、安全审计、终端防护等进行全面覆盖。通过准入控制，用户可以实时看到接入网络中的终端，并对这些终端进行准入控制；通过建立安全策略进行安全管理，系统可以感知到终端接入位置的变化以及类型信息变化；通过智能识别，用户可以感知接入网络中的终端类型，通过终端管理系统对网络中的终端进行高效的管理。

参考文献

[1] 数字时代关注终端安全[J].中国信息化，2021(4)：40.
[2] 闫珂.关于网络安全等级保护 2.0 的探讨[J].网络空间安全，2021，12(Z3)：11-14.
[3] 张敏莉.计算机终端安全管理策略及应用的研究[J].电脑知识与技术，2010，6(15)：3917-3918.
[4] 崔谊.网络发展给终端带来什么?[J].中国计算机用户，1996(5)：18-19.
[5] 臧璆.终端安全准入控制在网络安全中的应用分析[J].福建电脑，2020，36(10)：4.
[6] 王铭.一种终端类型识别方法及装置.中国：CN1093477-85A[P].2019-02-15.
[7] 高荣亮，郑乐.高可用 SDN 控制器主从分布式系统设计[J].光通信技术，2021，45(7)：59-62.
[8] 王胜志，章道勇.SD-WAN 网络架构及产品应用探索[J].邮电设计技术，2021(3)：71-76.
[9] 迈普通信技术股份有限公司.迈普金融办公网哑终端管控方案[J].中国金融电脑，2021(8).
[10] 康雅萍，陈熠，白浩.基于多域网络环境的终端安全管理体系的研究[J].长江信息通信，2021(6)：127-129.
[11] 赵华，周富林，黄靖.基于物联网终端管理云平台的大数据运维[J].现代传输，2021(2)：38-41.
[12] 张雪.5G 核心网云网一体化运维[J].电信科学，2021(8)：128-135.

(收稿日期：2021-10-31)

作者简介：

陆良伟(1994-)，男，硕士研究生，工程师，主要研究方向：物联网智能终端安全管理技术。

岳峙君(1998-)，女，本科，主要研究方向：物联网智能终端安全管理技术。

袁懿(1988-)，男，本科，主要研究方向：园区网细分场景整体解决方案技术。

扫码下载电子文档

版权声明