学校编码：10384　　分类号_____密级_____
学号：X2013231808　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

公司员工上网行为监管系统设计与实现

Design and Implementation of Company Employee Internet Behavior Supervision System

郭扬帆

指 导 教 师： 王美红助理教授

专 业 名 称： 软 件 工 程

论文提交日期： 2015 年 10 月

论文答辩日期： 2015 年 11 月

学位授予日期： 2015 年 12 月

指 导 教 师：_____

答辩委员会主席：_____

2015 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行)》。

另外,该学位论文为(　　)课题(组)的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。(请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。)

声明人（签名)：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

随着计算机技术的普及和公司办公的科技化发展，计算机正在不断进入越来越多的公司办公环境中。计算机的普及使得公司员工的办事效率大幅提高的同时，也带来了一些负面问题。不少员工在上班期间 QQ 聊天、淘宝、炒股、看视频、联网玩游戏等等，严重损坏了公司的形象，造成公司资源的浪费。因此，公司亟需要一种上网行为监管系统，来监督和管理员工在上班期间的上网行为，使得员工在上班期间不敢也不能使用计算机做与工作无关的事情。

本论文的研究是如何开发一个监管公司员工上网行为的系统，用于纠正公司员工使用计算机做其他事情的不良风气， 提升公司的形象，提高员工工作效率，实现公司计算机资源和网络资源的有效利用，并辅助公司领导了解员工上班期间的表现。

已有的公司员工上网行为监管系统，对公司员工上网行为的监管主要有物理监管、权限监管、时间监管、内容监管和审计报表监管等形式；对公司员工上网行为的控制主要有端口控制、IP 地址控制、URL 控制和应用层协议控制等。

本文围绕公司员工上网行为监管系统的设计与实现，对国内外的研究现状进行了研究，阐述了研究背景和意义，并提出了对建立公司员工上网行为监管系统的解决方案，通过系统需求分析，系统总体设计，系统详细设计与实现，系统测试，本课题实现了公司员工上网行为监管系统的基本功能。本系统的基本功能模块有协议分析模块，上网行为管控模块，流量统计模块，策略管理模块，系统管理模块和数据查询模块等。本课题以软件工程中软件生命周期为指导思想进行展开，用到的主要技术有协议分析技术，基于 URL 黑白名单的访问控制技术，基于 MySql 的数据库技术以及其他相关技术。

关键词：协议分析；流量统计；访问控制

Abstract

With the popularization of computer technology and the development of office science and technology, computer is constantly entering more and more company office environment. The popularization of computer makes the efficiency of the company staff greatly improved, but also brings some negative questions. Many employees QQ chat, Taobao shopping, stock, watch videos, play networking games during working time, Seriously damage the image of the company, resulting in the waste of company resources. Therefore, companies need an Internet behavior monitoring system, to supervise and manage the online behavior of employees during working time. So that employees can't use the computer to do nothing to do with work during the work.

This thesis researches on how to develop a company employee Internet behavior supervision system, which is used to correct the bad mood of the company employees using computer to do other things, enhance the company's image, Improve employee productivities, realize the effective use of computer resources and network resources, And assistant to the company leadership to understand the performance of the staff during the work.

Existing company employees online behavior monitoring system, the regulation of the Internet behavior of employees is mainly in the form of physical supervision, the authority supervision, the supervision of the time, the content and the audit report. The control of the Internet behavior of the employees of the company mainly includes port control, IP address control, URL control and application layer protocol control.

This thesis focuses the design and implementation of the Internet behavior supervision system for the employees of the company, has carried on research status at home and abroad, describes the research background and significance, and proposes some solutions to the establishment of the behavior supervision system for the employees of the company, through the system needs analysis, the system overall design, the system detailed design and the realization, the system test, this thesis has realized the basic function of the company employee net behavior supervision system. The basic function of this system is protocol analysis module, Internet behavior control module, traffic statistics module, policy management module, system management module, etc. This thesis carries on the development of the guiding

ideology of the software life cycle in the software engineering. The main technology used are protocol analysis technology, the URL black and white list of access control technology, MySql database and other related technologies.

Key Words: Protocal Analysis, Traffic Statistics, Access Control.

目 录

Contents

第1章 绪论

1.1 研究背景和意义

计算机的大量使用在给公司带来强大发展动力的同时，也为公司的管理者带来了不少困扰。一些员工工作期间联网玩游戏、迅雷下载电影、看网络视频、浏览博客、淘宝购物、炒股票、网上聊天等等，这些不仅会降低员工的工作效率，损害公司的外在形象，还造成了公司网络资源的巨大损耗，影响公司正常业务的运转。更为严重的是部分员工未经允许私自将公司的重要信息、文档等发布到互联网或者通过邮箱向外传递，造成公司机密信息的泄露。在这种背景下，迫切需要公司对员工上网行为进行监督和管理。

公司员工上网行为监管系统是根据对公司员工上网行为监管的实际需求所做的研究课题，系统通过对公司网络流量的分析、管控、统计，做到合理利用公司网络资源，提高公司员工工作效率，降低公司安全风险，辅助公司领导了解员工上班期间表现。

1.2 研究现状

1.2.1 员工上网行为监管形式

针对公司员工上网行为监管，形式上主要有物理监管、时间监管[1]、权限监管[2]、审计报表监管[3]等。

物理监管：对于需要使用计算机办公的员工给予配备电脑，对于不需要进行网络办公的员工，不配备计算机。

时间监管：把每天的时间根据工作和休息时间进行划分，在工作时间不提供网络服务，在休息时间提供网络服务。

权限监管：根据员工的级别和工作性质确定是否给员工开启互联网使用权限。

审计报表监管[4]：使用网络管理系统软件[5]，对员工的上网行为进行审计[6]、分析并生成统计报表，供领导参考。

1.2.2 员工上网行为访问控制

公司员工对互联网资源（网页、网络应用）的访问控制，主要分为以下四种。

基于IP地址的访问控制[7]，当数据包经过访问控制系统时，访问控制系统会分析所拦截的数据包是否属于IP协议。如果是，则根据IP协议从数据包中解析出目的IP地址，如果该目的IP地址位于IP地址黑名单中，则阻止该数据包；如果该目的IP地址位于IP地址白名单中，则直接放行；。如果既不在IP地址黑名单也不在IP地址白名单中，则采用默认控制策略。

基于端口的访问控制[8]，当数据包经过访问控制系统时，访问控制系统会分析所拦截的数据包是否属于TCP/UDP协议。如果是，则根据TCP/UDP协议从数据包中分析出目的端口，然后在已创建的端口过滤列表中查找该端口，如果发现该端口属于禁止访问端口，则对此次访问进行阻断，否则直接放行。

基于URL的访问控制[9]，当数据包经过访问控制系统时，访问控制系统会分析所拦截的数据包是否属于HTTP协议。如果是，则根据HTTP协议从数据包中分析出目的URL地址。查找URL黑白名单列表，如果发现目的URL地址位于URL黑名单列表中，则直接阻断该数据包；如果发现目的URL地址位于URL白名单列表中，则直接放行；如果既不在URL黑名单和URL白名中，则采用默认控制策略。

基于应用层协议的访问控制[10]，当数据包经过访问控制系统时，访问控制系统会对数据包进行逐层解析，得到数据包的目的 IP 地址、目的端口号、URL 地址、HOST 信息、UserAgent 信息，以及应用层协议中包含的与应用协议相关联的特征信息等， 综合利用这些信息得到数据包所归属的应用层协议类型，查找应用协议黑名单列表，如果发现应用协议类型位于应用协议黑名单列表中，则禁止访问，否则直接放行。

1.3 主要研究内容

本文设计并实现一个公司员工上网行为监管系统。为企业管理人员监管员工上网行为提供一个简单、实用、高效的平台。

首先，本系统实现了基于 URL 黑白名和应用层协议类型的访问控制，用于管控和约束员工工作期间的上网行为。

其次，本系统提供了用于员工上网流量统计的平台，可以根据各种条件对公

司、部门、员工的历史上网行为进行统计与展示。

第三，本系统可以查询员工上网行为过滤日志以及员工上网行为 TOPN 信息，帮助公司领导了解员工试图访问哪些不允许访问的网站和应用，进而掌握工作期间公司计算机和网络资源的有效使用率。

1.4 论文结构安排

第一章，对公司员工上网行为监管系统的研究意义、研究现状以及研究内容做了介绍；

第二章，对公司员工上网行为监管系统所需要的相关技术进行了介绍，如 LIBPCAP 数据包捕获，OSI 七层协议模型、URL 黑白名单过滤，应用软件过滤等；

第三章，对公司员工上网行为监管系统做了需求分析；

第四章，利用图文方式描述说明公司员工上网行为监管系统设计；

第五章，描述了公司员工上网行为监管系统的开发相关的实现过程；

第六章，描述了公司员工上网行为监管系统的测试环境和系统的容错测试；

第七章，对公司员工上网行为监管系统进行总结，同时对不足的部分进行展望。

第2章 相关技术介绍

本系统涉及的技术主要有 libpcap 数据包捕获、OSI 七层协议模型、URL 黑白名单过滤、应用软件过滤、Netflow 流量统计、Brower/Server 架构等。

2.1 Libpcap 数据包捕获

Libpcap[11]提供了用户可以调用的网络数据包捕获接口，并具备很强的可移植性。Libpcap 可以在绝大多数 Linux 平台上运行，工作在上层应用程序与网络接口之间。其主要功能有数据包捕获、自定义数据包发送、流量采集与统计、规则过滤等。其工作流程如图 2-1 所示。

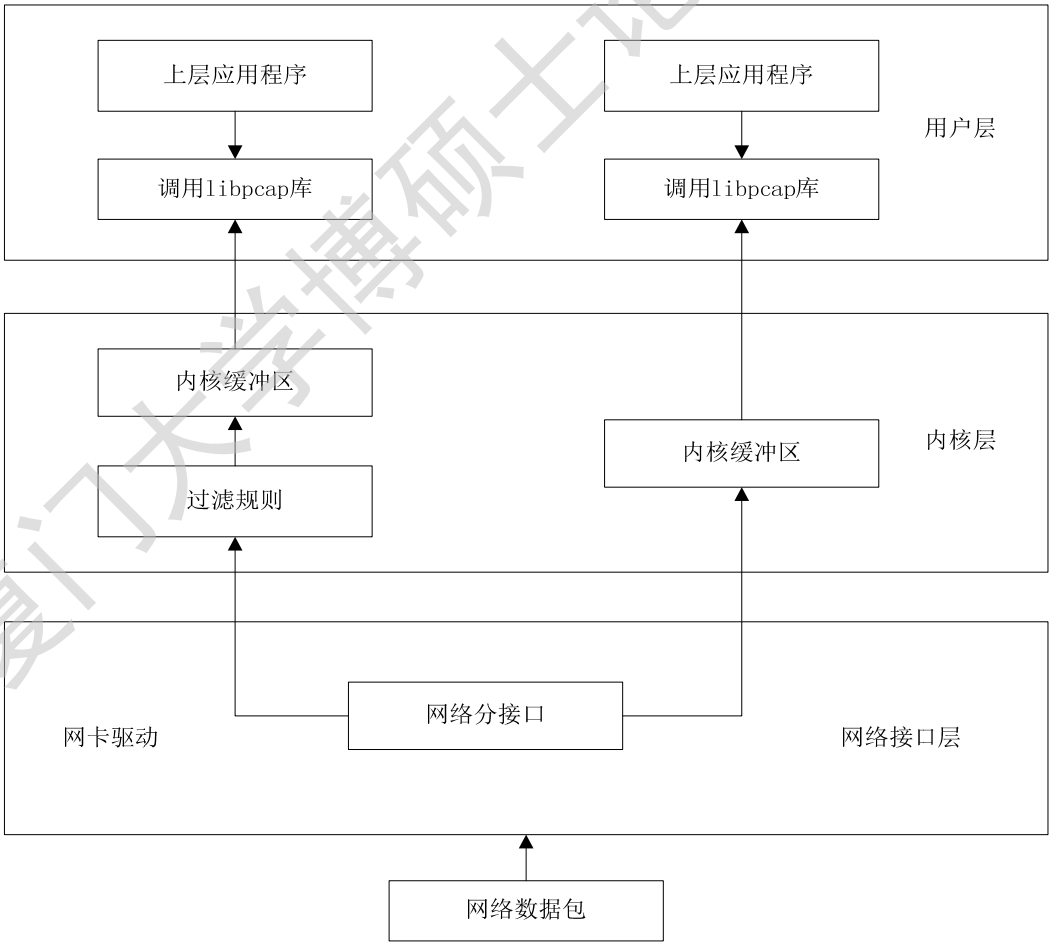

图 2-1 libpcap 工作流程

2.2 OSI 七层协议模型

OSI 七层协议模型[12]如图 2-2 所示。

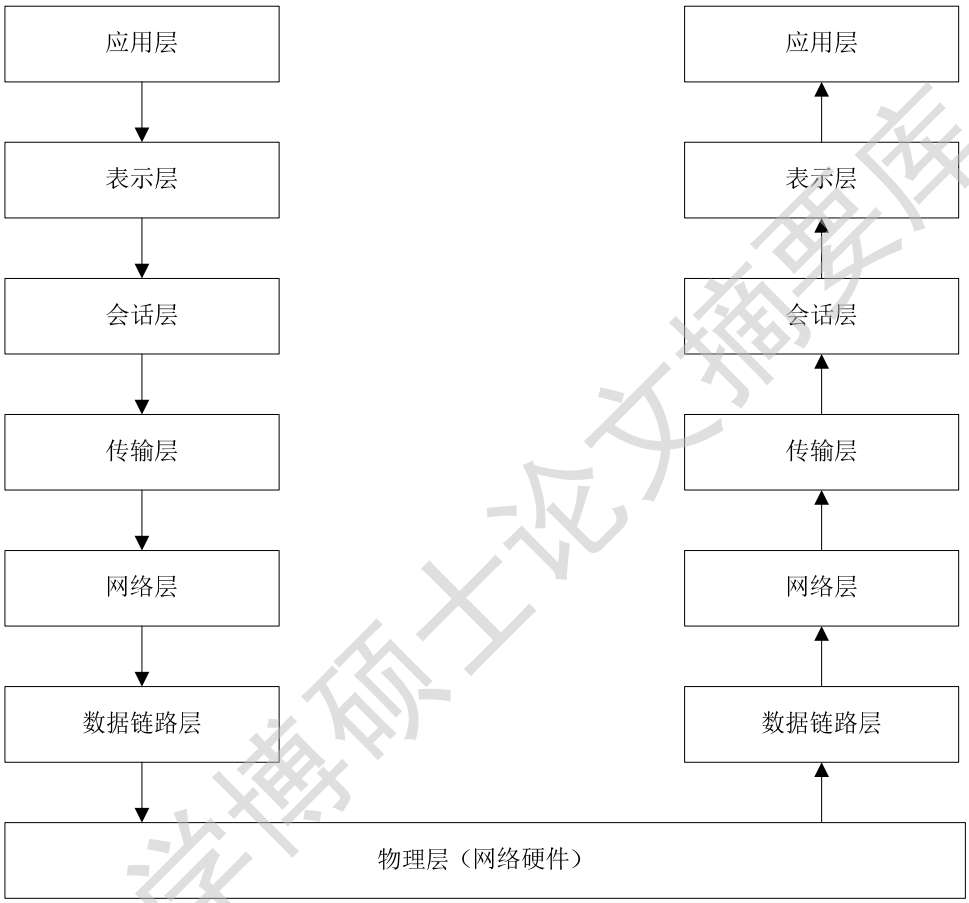

图 2-2 OSI 七层模型

应用层产生的数据在通过物理网络传输之前，按照 OSI 七层模型，从上到下逐层封装，每一层都分别将接收到的数据包前面加上本层的报文头部，最后封装后的数据包通过物理网络传输到目的网络。当数据包到达目的网络后，再从下到上，对数据包逐层解封装，在每一层分别去掉本层的数据包头部，在到达应用层后，用户获得原始数据。

2.3 URL 黑白名单过滤

URL 黑白名单过滤是实现网页访问控制最常用的技术之一[13]。URL 黑白名单是 URL 黑名单和 URL 白名单的统称。URL 黑名单中存放的是禁止用户访问