



(12) 发明专利申请

(10) 申请公布号 CN 103873285 A

(43) 申请公布日 2014. 06. 18

(21) 申请号 201210549100. 0

(22) 申请日 2012. 12. 18

(71) 申请人 河南省电力公司郑州供电公司

地址 450006 河南省郑州市淮河路 9 号

申请人 国家电网公司

(72) 发明人 周楠 吴晖 车志超 刘伯宇

耿芳 王然 王宇 李璨

(74) 专利代理机构 郑州中原专利事务所有限公

司 41109

代理人 张春 李想

(51) Int. Cl.

H04L 12/24 (2006. 01)

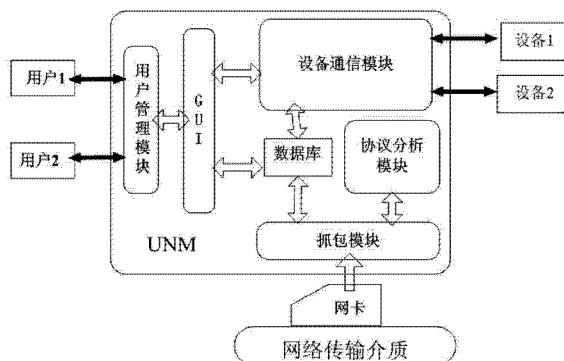
权利要求书1页 说明书3页 附图3页

(54) 发明名称

信息网络统一管理平台

(57) 摘要

一种信息网络统一管理平台，它包括：图形化操作界面，网管用户使用图形化操作界面和 UNM 交互，UNM 依据用户请求完成指定操作，并通过 GUI 进行回显；用户管理模块对各个网管用户分级管理，所有运维人员共享网络管理及维护信息，数据的更改对所有运维人员可见；设备通信模块，UNM 服务端使用通信模块同网络交换设备通信，完成数据传输或压缩、加密及认证操作；抓包模块，负责监听网络数据包，所捕获的数据包经由协议分析模块处理之后生成统计数据交给图形化操作界面呈现。采用上述技术方案的本发明，基于网络嗅探、协议分析、网络安全协议、数据库等技术，搭建统一的信息及设备管理平台，并提供网络故障诊断支持，提高运维效率。



1. 一种信息网络统一管理平台,其特征在于,它包括 :

图形化操作界面,网管用户使用图形化操作界面和 UNM 交互,UNM 依据用户请求完成指定操作,并通过 GUI 进行回显;

用户管理模块,对各个网管用户分级管理,所有运维人员共享网络管理及维护信息,数据的更改对所有运维人员可见;

设备通信模块,UMN 服务端使用通信模块同网络交换设备通信,完成数据传输或压缩、加密及认证操作;

抓包模块,负责监听网络数据包,所捕获的数据包经由协议分析模块处理之后生成统计数据交给图形化操作界面呈现。

2. 根据权利要求 1 所述的信息网络统一管理平台,其特征在于 : UNM 使用抓包模块在核心交换设备上进行嗅探,对网络流量及数据包协议进行分析,将网络流量及数据包协议信息定位到单个 IP 或 MAC。

3. 根据权利要求 2 所述的信息网络统一管理平台,其特征在于 : UNM 的网络嗅探功能基于 Winpcap 实现 ;所述的 Winpcap 由三部分组成 :一个数据包截获驱动程序、一个底层动态链接库和一个高层静态链接库 ;其嗅探过程为 :将获取的数据包进行过滤后,进行读取和解析。

4. 根据权利要求 3 所述的信息网络统一管理平台,其特征在于,协议分析模块的处理过程是 :对于嗅探过程中抓取到的每一个数据包,依次剥去 Winpcap 头和 MAC 头,并判断是否为 IP 包 ;如果是 IP 包,则解析 IP 头并判断是否为 TCP 包,如果是 TCP 包,则解析 TCP 头并判断是否为 HTTP 包,如果是 HTTP 包,则解析 HTTP 头。

信息网络统一管理平台

技术领域

[0001] 本发明涉及一种信息及设备管理平台。

背景技术

[0002] 信息技术的发展和应用是建设坚强智能电网的必要前提,信息网络则是信息技术应用的基础。目前,郑州供电公司已经建成计算机千兆光纤城域专用数据网络,形成了以千兆光纤为主干、百兆交换到桌面的“信息高速公路”,公司信息网络成为信息业务传输的可靠平台。随着公司网络规模不断扩大,截止到 2010 年 12 月,公司信息内网已经覆盖公司 14 个机关部室、28 个二级单位、6 县(市)电业局、106 座变电站和 8 个营业所,网络跨度达 100 公里以上,联网业务终端 3000 余台。业务多、设备多、用户多、地域广是公司信息网络的主要特点,而信息业务的持续拓展、网络用户的迅速增加,以及网络规模的逐渐扩大,使得网络运维管理工作日益繁重。

[0003] 目前我公司在网络运维管理上缺少自动化的辅助工具,工作繁琐且效率不高。例如,新增网络用户时,网络运维管理人员需要首先依据用户所属部门查找到其部门 IP 段,然后查找该部门的地址绑定交换机 IP,然后登录交换机找出可用 IP,并将用户 MAC 地址和 IP 进行绑定,最后将新增用户的信息登记备案。以上操作过程繁琐且具有重复性,同时,因调整工位或部门导致用户信息频繁变更、不同运维人员信息难以及时共享造成运维资料的偏差,以及空闲 IP 地址难以及时回收使得 IP 资源日益紧张等等,都是网络运维管理工作必须面对并尽快解决的问题。

发明内容

[0004] 本发明的目的是提供一种管理统一、提高工作效率的信息网络统一管理平台。

[0005] 为实现上述目的,本发明采用以下技术方案:

一种信息网络统一管理平台,它包括:

图形化操作界面,网管用户使用图形化操作界面和 UNM 交互,UNM 依据用户请求完成指定操作,并通过 GUI 进行回显;

用户管理模块,对各个网管用户分级管理,所有运维人员共享网络管理及维护信息,数据的更改对所有运维人员可见;

设备通信模块,UMN 服务端使用通信模块同网络交换设备通信,完成数据传输或压缩、加密及认证操作;

抓包模块,负责监听网络数据包,所捕获的数据包经由协议分析模块处理之后生成统计数据交给图形化操作界面呈现。

[0006] UNM 使用抓包模块在核心交换设备上进行嗅探,对网络流量及数据包协议进行分析,将网络流量及数据包协议信息定位到单个 IP 或 MAC。

[0007] UNM 的网络嗅探功能基于 Winpcap 实现;所述的 Winpcap 由三部分组成:一个数据包截获驱动程序、一个底层动态链接库和一个高层静态链接库;其嗅探过程为:将获取的

数据包进行过滤后,进行读取和解析。

[0008] 协议分析模块的处理过程是:对于嗅探过程中抓取到的每一个数据包,依次剥去Winpcap头和MAC头,并判断是否为IP包;如果是IP包,则解析IP头并判断是否为TCP包,如果是TCP包,则解析TCP头并判断是否为HTTP包,如果是HTTP包,则解析HTTP头。

[0009] 采用上述技术方案的本发明,基于网络嗅探、协议分析、网络安全协议、数据库等技术,搭建统一的信息及设备管理平台,并提供网络故障诊断支持,提高运维效率。具有以下优点:

1、搭建统一的信息管理平台,实现运维人员之间的信息共享;

2、设计一致的设备管理及操作界面,屏蔽因设备类型不同带来的配置命令差异性,简化操作;

3、提供网络故障诊断支持,减少工作量,提高运维效率。

附图说明

[0010] 图1为本发明的原理框图。

[0011] 图2为本发明中UNM网络嗅探模块工作原理图。

[0012] 图3为UNM协议解析流程图。

具体实施方式

[0013] 本发明中,基于网络嗅探、协议分析、网络安全协议、数据库等技术,搭建统一的信息及设备管理平台,并提供网络故障诊断支持,提高运维效率。

[0014] 如图1所示,一种信息网络统一管理平台,它包括:

网管用户使用图形化操作界面GUI和UNM交互,UNM依据用户请求完成指定操作,并通过GUI进行回显。

[0015] UNM用户管理模块对各个网管用户分级管理,所有运维人员共享网络管理及维护信息,数据的更改对所有运维人员可见,有效避免因信息不一致而造成的管理维护混乱。

[0016] 在设备管理方面,UNM服务端使用通信模块同网络交换设备通信,完成简单数据传输(基于telnet协议)或压缩、加密及认证(基于SSH/SSH2协议)操作。一方面,屏蔽了网络设备间通信协议的差异,为用户提供了一个一致的配置平台而无需再针对不同设备使用不同的配置工具;另一方面,UNM采用统一的GUI,屏蔽了不同型号网络设备(CISCO、H3C等)控制命令的差异,使得需要手工键入若干复杂命令的配置工作只需点击相应任务按钮即可完成,大大简化了运维人员的配置操作。

[0017] 抓包模块是流量统计功能模块的基础,负责监听网络数据包,所捕获的数据包经由协议分析模块处理之后生成统计数据交给GUI呈现。在网络故障诊断方面,UNM使用抓包模块在核心交换设备上进行嗅探,对网络流量及数据包协议进行分析,将网络流量及数据包协议信息定位到单个IP或MAC,提供针对单台计算机的网络数据监测,不但可以及时发现、回收不使用的IP地址,也可对局域网病毒的防治提供诊断支持。

[0018] 其中,UNM在Visual Studio 2008下基于MFC框架实现。主界面为MDI结构,各个功能模块依托FormView实现,分别对应于类CMainFormView(信息查询模块)、CChildView_FlowStatis、CChildView_EquipmentStatis、CChildView_EquipmentDetail

(使用 CxSplitterWnd 类左右拆分为 CChildView_EquipmentDetail_LeftTreeView 和 CChildView_EquipmentDetail_RightFormView)。各个视图类负责响应所含窗体控件消息，主框架类响应系统菜单及工具栏消息。

[0019] 考虑到设备登录功能的实现需要依托窗体控件进行，故直接由 MFC 的窗体控件类 CEdit 派生出具有网络交互功能的 CEdit_ZN 类以实现命令行模式登录设备。我公司现有网络设备的链接协议有两种，Telnet 和 SSH2。telnet 为熟知协议，查阅 RFC 854 或其他相关资料即可完成代码编写。SSH2 是一套商业化的安全通讯协议框架，其设计实现较为复杂且不开源，故 UNM 的 SSH2 通信过程基于 libssh2 实现。libssh2 是 linux 平台下的一个 C 函数库，用来实现 SSH2 协议。在 windows 上利用这些库需要自己编译 SSH2 库并集成到 IDE 中。

[0020] 如图 2 所示，UNM 的网络嗅探功能基于 Winpcap 实现。Winpcap (Windows Packet Capture) 是一个免费的网络驱动开发包，是由 UNIX 平台下的 libpcap 函数库移植到 Windows 上所得，提供功能强大的数据包分组捕获机制，为 win32 应用程序提供访问网络底层的能力。Winpcap 由三部分组成：一个数据包截获驱动程序、一个底层动态链接库(packet.dll)和一个高层静态链接库(wpcap.lib)，由于它工作于驱动层、效率很高。Winpcap 提供的功能包括：捕获网络原始数据包、把数据包写入到文件并从文件中读出、自定义数据包的过滤策略、发送原始数据包、收集网络统计信息。使用 Winpcap，可以很方便的编写出用于网络协议实验分析、故障诊断、网络安全和监视等方面的应用程序。

[0021] 如图 3 所示，UNM 嗅探器启动后，查找并列出网络设备，依据用户选择打开指定网卡，然后启动截包线程。对于嗅探器抓取到的每一个数据包，UNM 协议分析模块就按照图 3 所示流程依据匹配端口及数据包协议字段的方法进行解析，并将解析结果显示在 GUI 中或记录到数据库中。具体的解析过程为：对于嗅探过程中抓取到的每一个数据包，依次剥去 Winpcap 头和 MAC 头，并判断是否为 IP 包；如果是 IP 包，则解析 IP 头并判断是否为 TCP 包，如果是 TCP 包，则解析 TCP 头并判断是否为 HTTP 包，如果是 HTTP 包，则解析 HTTP 头。

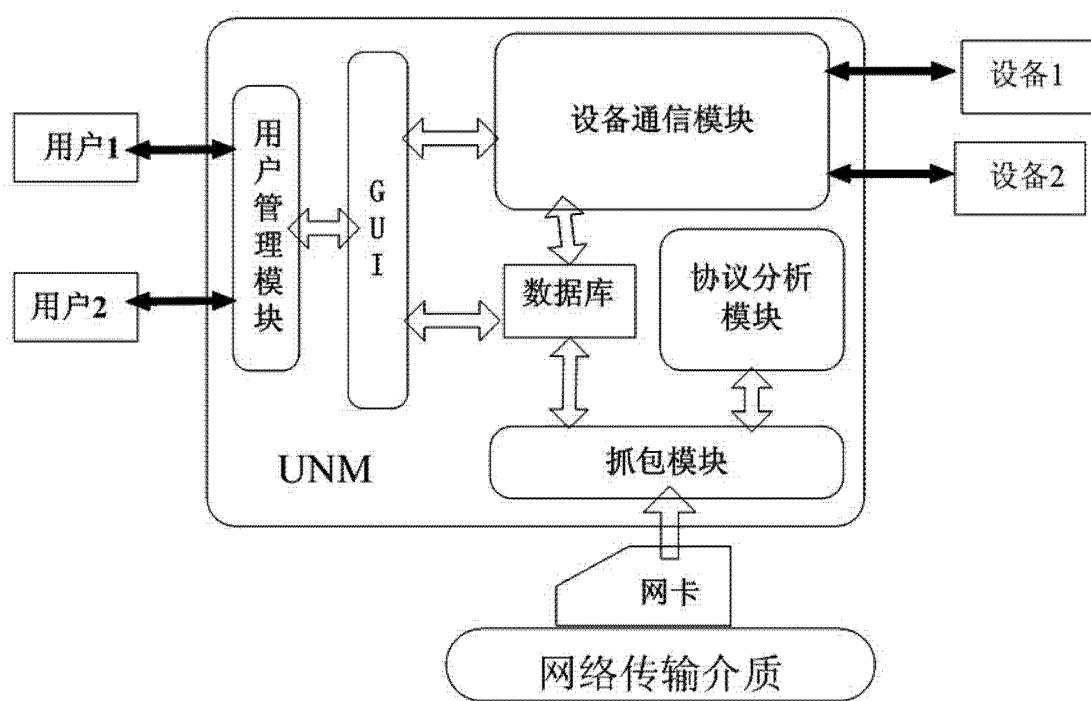


图 1

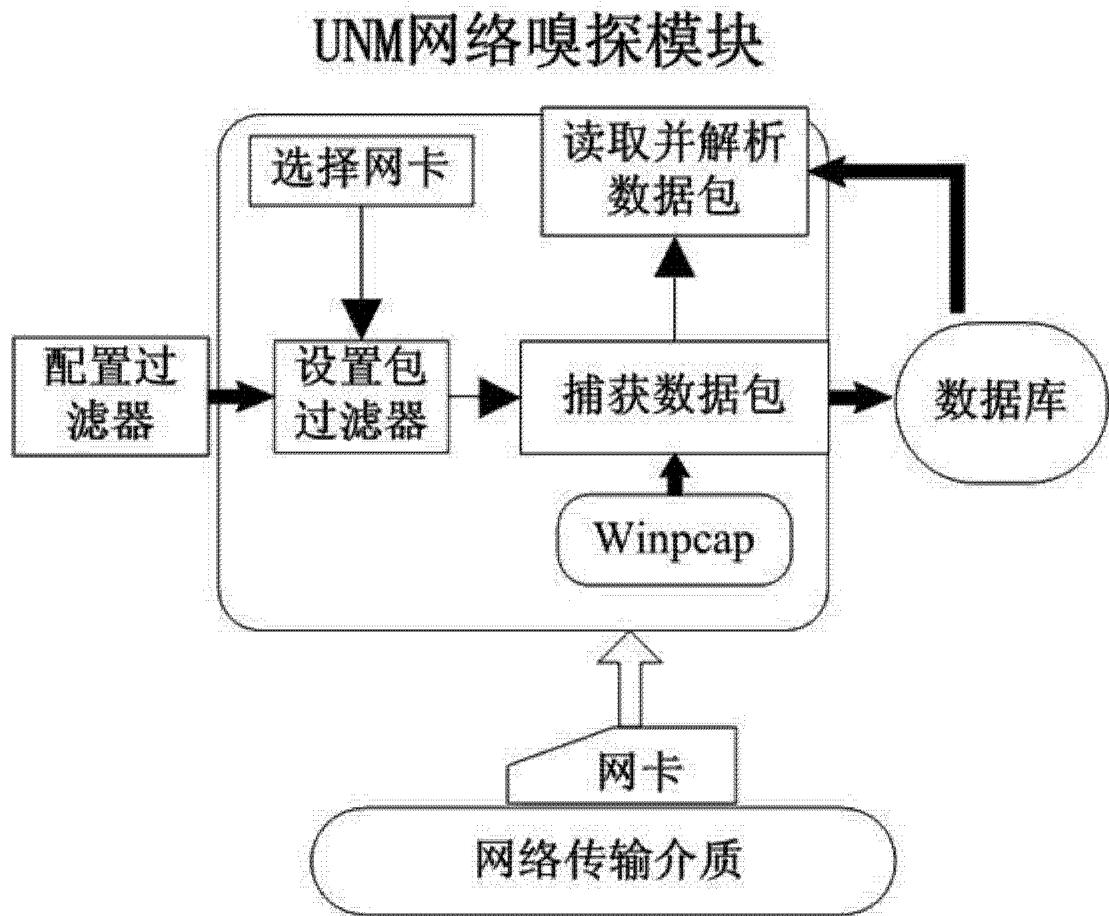


图 2

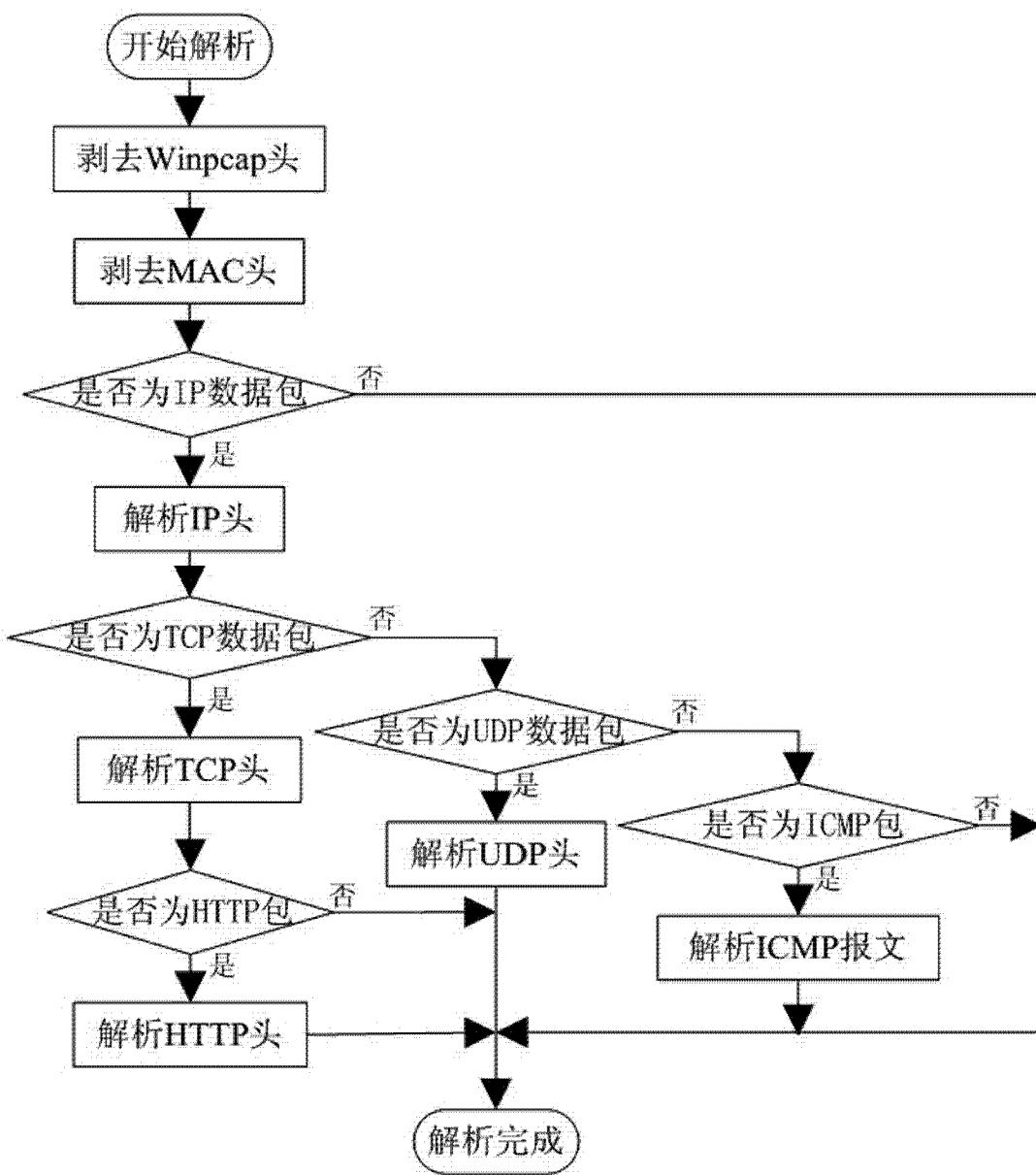


图 3