[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/56 (2006.01)
H04L 12/24 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410084539.6

[45] 授权公告日 2007 年 6 月 13 日

[11] 授权公告号 CN 1321516C

[22] 申请日 2004.11.25
[21] 申请号 200410084539.6
[73] 专利权人 上海复旦光华信息科技股份有限公司
地址 200433 上海市杨浦区国泰路 127 号 3 号楼
[72] 发明人 张世永 严 明 郭 巍
[56] 参考文献
US5218603A 1993.6.8
CN 1516386A 2004.7.28
CN14350758A 2003.10.22
基于骨于网的并行集群入侵检测系统 杨武，方滨兴，云晓春，张宏莉,哈尔滨工业大学学报,第 36 卷第 3 期 2004
基于数据分流实现高速网入侵检测的研究与实践 朱奋起，陈宇，李雪莹，许榕生,计算机应用研究,第 5 卷 2004
利用分割机制实现高速网下入侵检测的研究 薛华，李祥和，许榕生,计算机工程,第 30 卷第 3 期 2004
利用数据分流实现高速网下入侵检测的研究与实现 薛华，李雪莹，陈宇，许榕生,计算机应用研究,第 5 卷 2004
审查员 胡锐先
[74] 专利代理机构 上海交达专利事务所
代理人 王锡麟 王桂忠

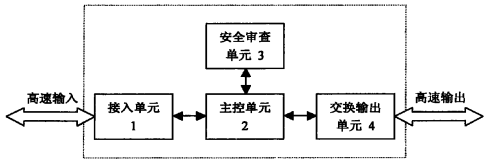
权利要求书 2 页 说明书 6 页 附图 3 页

[54] 发明名称

基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器

[57] 摘要

一种基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器，由接入单元、主控单元、安全审查单元、交换输出单元组成，接入单元与主控单元互连，主控单元与交换输出单元互连，安全审查单元与主控单元互连，其中，接入单元由 10G 光电信号转换模块，2.5G POS 光电信号转换模块和成帧芯片组成，主控单元由网络处理器单元和 4 路千兆物理接口组成，安全审查单元由 4 个带千兆电口接口的标准 CPU 处理模块组成；交换输出单元由千兆交换主控模块、千兆电口接口模块、千兆光口接口模块组成，安全审查单元将检查结果反馈给主控单元，主控单元根据细粒度过滤结果为该数据包制定分流策略，并将制定好的数据分流策略下发给交换输出单元执行具体的数据转发操作。



1、一种基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器，由接入单元、主控单元、安全审查单元、交换输出单元组成，其特征在于，接入单元与主控单元互连，主控单元与交换输出单元互连，安全审查单元与主控单元互连，

其中：所述的接入单元由 10G 光电信号转换模块，2.5G POS 光电信号转换模块和成帧芯片组成，10G 光电信号转换模块和 2.5G POS 光电信号转换模块分别通过 SFI 接口与成帧芯片连接，成帧芯片通过高速 SPI-4.2 接口与主控单元连接；

所述的主控单元由网络处理器单元和 4 路千兆物理接口组成，网络处理器单元包括帧头信息处理模块、分类查找处理模块、转发决策处理模块，帧头信息处理模块通过 SPI-4.2 接口与接入单元相连，分类查找处理模块与帧头信息处理模块相连，转发决策处理模块与分类查找处理模块相连，转发决策处理模块通过 GMII 接口与安全审查单元相连，转发决策处理模块通过 XAUI 与交换输出单元相连；

所述的安全审查单元由 4 个带千兆电口接口的标准 CPU 处理模块组成，安全审查单元对在所述主控单元中标记为“细粒度处理”的数据包进行细粒度处理，并将此细粒度处理结果反馈给主控单元，主控单元根据此细粒度处理结果为对应数据包制定分流策略，并将制定好的数据分流策略下发给交换输出单元执行具体的数据转发操作；

所述的交换输出单元由千兆交换主控模块、千兆电口接口模块、千兆光口接口模块组成，交换输出单元共 8 个千兆电口和 4 个千兆光口，千兆交换主控模块通过 GMII 接口分别与千兆电口接口模块和千兆光口接口模块相连。

2、根据权利要求 1 所述的基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器，其特征是，所述的 10G 光电信号转换模块，其兼容 10G POS、10G LAN、WAN。

3、根据权利要求 1 所述的基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器，其特征是，所述的接入单元，对来自网络中各种类型的数据流进行光电转换、串/并转换，帧处理，按照 PPP/HDLC Over SONET/SDH 协议规范从 SONET/SDH 将数据流还原为 PPP 数据包，然后通过高速 SPI-4.2 接口传递给主控单元处理。

4、根据权利要求 1 所述的基于网络处理器和 CPU 阵列的交换架构的安全过滤

分流器，其特征是，所述的主控单元，主要负责对接入单元接收并处理过的数据包进行粗过滤和数据分流策略的判定。

5、根据权利要求 1 所述的基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器，其特征是，所述的帧头信息处理模块，按照标准协议规范检验接入单元发送过来的数据包的完整性并处理基本的协议连接。

6、根据权利要求 1 所述的基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器，其特征是，所述的分类查找处理模块，按照预先设置的过滤规则对数据包进行七层线速匹配，过滤项主要依据七层协议的头信息进行过滤，属于粗粒度过滤，主要的过滤项包括：规则号、源 MAC 地址、目的 MAC 地址、源 IP 地址、源 IP 掩码、目的 IP 地址、目的 IP 掩码、源端口号、目的端口号、URL 地址、相应过滤操作，其中“相应过滤操作”选项中包括细粒度处理、丢弃、转发三种选择，分类查找处理模块根据规则匹配结果，过滤掉标签为“丢弃”的非法数据包和异常数据包，将需要进一步细粒度处理的数据包和直接转发数据包分别打上“细粒度处理”标签和“转发处理”标签，发送到转发决策处理模块。

7、根据权利要求 1 所述的基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器，其特征是，所述的转发决策处理模块，将标签为“细粒度处理”的数据包通过内置的千兆口转发到安全审查单元，将标签为“转发处理”的数据包按通用负载均衡算法进行分发策略的计算，保证所有的数据在任意一条链路上保持其 TCP 完整连接，转发决策处理模块将计算得到的分发策略通过 SPI-4.2 接口发送到交换输出单元。

8、根据权利要求 1 所述的基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器，其特征是，所述的 4 个标准 CPU 处理模块，采用并行处理的工作模式，实现对数据包内容的细粒度检查，细粒度检查根据待细粒度检查的应用的应用层协议规范中的定义，通过设置要匹配内容的字段偏移量、字段长度、字段内容以及过滤操作，利用关键字匹配的方法对数据包进行内容审查，安全审查单元基于会话的数据包内容审查，将从一个会话中的多个数据包提取出的信息进行拼接，再进行内容匹配，发现分散在多个数据包中的情况。

基于网络处理器和CPU阵列的交换架构的安全过滤分流器

技术领域

本发明涉及一种高速网络流量环境下的数据处理装置，特别是一种基于网络处理器和CPU阵列的交换架构的安全过滤分流器，用于网络信息技术领域。

背景技术

近年来，我国在宽带骨干网络方面的发展较快，目前大部分区域骨干网的带宽达到2.5G，部分骨干网的带宽达到10G甚至40G。从过去近10年互联网的发展来看，处理器的速度每18个月翻一番，但互联网骨干连接的带宽每12个月就要翻一番。可见，如何基于现有处理器性能达到宽带网络的高速数据处理需求是保障网络服务质量的关键。负载均衡和数据分流技术是当前提高网络数据处理性能的一种解决方案，许多安全产品都借助这些技术来扩展服务器带宽和增加吞吐量。根据实现原理的不同，负载均衡和数据分流设备主要包括以下类型：

1．采用通用CPU（中央处理单元，或中央处理器或微处理器）配合软件的技术方案实现。这种基于X86单机和网卡的架构实现，由于受到CPU处理能力和PCI总线速度的制约，已经难以满足千兆以上骨干网络的高速数据处理需求。

2．采用ASIC（专用集成电路）实现。在高速数据处理方面，虽然ASIC仍是当前网络设备的主流处理核心技术，它通过把指令或计算逻辑固化到硬件中以实现很高的处理速度，从而很好满足了网络设备对性能的要求，但ASIC缺乏灵活性，研制周期长，研发费用高，前期投入风险高，特别是在数据“智能化处理”和对用户定制化服务方面有缺陷，成为限制其进一步发展的主要因素。

目前通常是将分发各种服务请求所需要的处理时间作为衡量负载均衡和数据分流设备的重要性能指标，而不关心这些请求数据包对后端处理器的安全性和有效性，事实上很多设备把大量的攻击包和无效数据包也都一并转发给了后端应用系统，这使得后端应用和安全系统不得不面对较大的数据处理负担和安全威胁。

经对现有技术文献的检索发现，朱奋起等人在《计算机应用研究》2004年vol.21，No.5，p.149-151上发表“基于数据分流实现高速网入侵检测的研究与实践”中，

提出一种数据分流的方法，将捕获的网络数据按某种规则分流转发至多台检测设备进行处理，以达到提高整个系统的检测性能，解决高速网络下网络入侵检测设备因性能缺陷而带来的丢包问题。但该文提出的分流设备采用普通 PC 机作为前端机，使用千兆网卡获取网络数据，是典型的“单机+网卡”的结构，仅适用于千兆网络环境，根本无法满足 10G 高流量网络环境下数据处理要求。由此可见，在网络带宽和安全威胁不断增加的情况下，对网络设备在数据转发处理上的实时性、安全性和有效性等方面都提出了更高的要求，而现有的技术和产品还无法满足宽带网络对海量数据处理提出的较高实时性和可靠性的要求。

发明内容

本发明的目的在于克服现有数据分流系统在宽带网络环境中存在的缺陷，提出一种基于网络处理器和 CPU 阵列的交换架构的安全过滤分流器。使其针对 10G 以上宽带网络环境下的数据处理需求，根据网络处理器和通用 CPU 处理器在海量数据处理上的特性，将对网络数据的过滤分流处理工作进行合理分解，对请求数据包在不同的处理器上进行分层次的数据转发处理和安全审查，使二种处理器能够充分地发挥各自的优势，并采用数据分流策略制定与数据转发相分离的架构，从而减轻了安全过滤分流器的核心处理单元的工作负担，在宽带网络环境下能够达到安全高效的数据过滤分流处理性能，能够为各种宽带网络应用提供较高的数据接入质量。

本发明是通过以下技术方案实现的，本发明由接入单元、主控单元、安全审查单元、交换输出单元组成，接入单元与主控单元互连，主控单元与交换输出单元互连，安全审查单元与主控单元互连。

接入单元由 10G（千兆位）光电信号转换模块，2.5G POS 光电信号转换模块和成帧芯片组成，10G 光电信号转换模块和光电信号转换模块不能同时使用，两种模块通过 SFI（并串 / 串并转换器和成帧芯片接口）和成帧芯片连接，成帧芯片通过高速 SPI-4.2（系统包接口 4.2 类型）接口与主控单元连接；所述 10G 光电信号转换模块可兼容 10G POS（基于同步数位阶层光纤网络的数据包）、10G LAN（局域网）、WAN（广域网络）。

接入单元对来自网络中各种类型的数据流进行光电转换、串/并转换，帧处理，按照 PPP/HDLC Over SONET/SDH（基于同步光网络协议/同步数位阶层光纤网络的点到点/高级数据链路控制）协议规范从 SONET/SDH（同步光网络协议/同步数

位阶层光纤网络）将数据流还原为 **PPP**（点到点协议）数据包，然后通过高速 **SPI-4.2** 接口传递给主控单元处理。

主控单元由网络处理器单元和 **4** 路千兆物理接口组成，网络处理器单元包括帧头信息处理模块、分类查找处理模块、转发决策处理模块；帧头信息处理模块通过 **SPI-4.2** 接口与接入单元相连，分类查找处理模块与帧头信息处理模块相连，转发决策处理模块与分类查找处理模块相连，转发决策处理模块通过 **GMII**（千兆位媒体独立接口）与安全审查单元相连，转发决策处理模块通过 **XAUI**（附件单元接口）与交换输出单元相连。

主控单元是本发明的核心处理单元，主要负责对接入单元接收并处理过的数据包进行粗过滤（通过预先设置粗粒度数据包内容检查规则）和数据分流策略的判定。

所述帧头信息处理模块按照标准协议规范检验接入单元发送过来的数据包的完整性并处理基本的协议连接；

分类查找处理模块按照预先设置的过滤规则对数据包进行七层线速匹配，过滤项主要依据七层协议的头信息进行过滤，属于粗粒度过滤，主要的过滤项包括：规则号、源 **MAC** 地址、目的 **MAC** 地址、源 **IP** 地址、源 **IP** 掩码、目的 **IP** 地址、目的 **IP** 掩码、源端口号、目的端口号、**URL** 地址、相应过滤操作，其中“相应过滤操作”选项中包括细粒度处理、丢弃、转发三种选择，分类查找处理模块根据规则匹配结果，过滤掉标签为“丢弃”的非法数据包和异常数据包，将需要进一步细粒度处理的数据包和直接转发数据包分别打上“细粒度处理”标签和“转发处理”标签，发送到转发决策处理模块；

转发决策处理模块将标签为“细粒度处理”的数据包通过内置的千兆口转发到安全审查单元，将标签为“转发处理”的数据包按通用负载均衡算法，如最小响应时间法，最小连接法进行分发策略的计算，要保证所有的数据在任意一条链路上保持其 **TCP** 完整连接，转发决策处理模块将计算得到的分发策略通过 **SPI-4.2** 接口发送到交换输出单元。

安全审查单元由 **4** 个带千兆电口接口的标准 **CPU** 处理模块组成，所述 **4** 个 **CPU** 处理模块采用并行处理的工作模式，实现对数据包内容的细粒度检查，大大提高了系统对数据包进行细粒度检查的处理效率。细粒度检查主要是针对不同种类应用的审查需要，根据应用层协议规范中的定义，通过设置要匹配内容的字段偏移量、字

段长度、字段内容以及过滤操作，利用关键字匹配的方法对数据包进行内容审查。安全审查单元具有基于会话的数据包内容审查功能，将从一个会话中的多个数据包提取出的信息进行拼接，再进行内容匹配，可以发现分散在多个数据包中的异常情况。安全审查单元将检查结果反馈给主控单元，主控单元根据细粒度过滤结果为该数据包制定分流策略，并将制定好的数据分流策略下发给交换输出单元执行具体的数据转发操作。

交换输出单元主要由千兆交换主控模块、千兆电口接口模块、千兆光口接口模块组成，交换输出单元共 **8** 个千兆电口和 **4** 个千兆光口，千兆交换主控模块通过 **GMII**（千兆位媒体独立接口）接口分别与千兆电口接口模块和千兆光口接口模块相连，交换输出单元根据主控单元制定的分发策略完成数据转发操作。

对局域网内的服务请求的转发处理，为了缓解主控单元的处理负担，主控单元仅对每个会话的第一个数据包进行数据分流策略的判定，对于属于同一个会话的后续数据包由交换输出单元根据主控单元制定并下发的转发策略执行具体的策略判断与数据转发处理操作。

本发明具有实质性特点和显著进步：（**1**）采用多级架构设计，将海量数据处理任务合理拆解，分配到不同的处理单元负责，缓解了核心的数据分流处理单元的工作压力，提高了系统整体的处理性能；（**2**）采用高性能的网络处理器技术实现数据分流处理，支持万兆的数据处理性能；（**3**）采用交换架构的设计，使局域网内的服务请求的数据分流策略的制定与数据转发的具体实施相分离，提高了系统核心处理单元的工作效率；（**4**）利用通用 **CPU** 阵列进行数据包内容的细粒度过滤，提高了所述安全过滤分流器在应用层的安全处理性能，使网络处理器能够更好的发挥其在网络层以下的包处理优势，深入的应用层数据分析提高了数据转发策略的安全性和有效性。

本发明提出的安全过滤分流器能够实现对 **2.5G**、**10G** 高流量背景下网络数据的线速无遗漏的获取，充分利用网络处理器技术结合通用处理器技术实现对数据包的七层线速预处理和智能的内容安全过滤，有效的解决了高速网络环境下对海量数据进行集群处理在实时性和安全性上的需求，适用于高速骨干网上的网络监测、入侵检测、流量统计、内容审计等多种安全应用的实施。

附图说明

图 1 本发明结构框图

图 2 接入单元组成结构框图

图 3 主控单元组成结构框图

图 4 安全审查单元组成结构框图

图 5 交换输出单元组成结构框图

具体实施方式

如图 1 所示，所述系统采用多路输入输出接口结构设计，接入单元 1 包括 2.5G POS 接口，10G POS 接口和千兆接口，接入单元 1 与主控单元 2 之间通过 SPI（系统包接口）总线互连，SPI 总线的带宽资源为 10G，主控单元 2 与安全审查单元 3 之间通过 PCI（外部设备接口）总线进行数据通信，PCI 总线的带宽资源为 1000MBps，主控单元 2 与交换输出单元 4 之间通过 SPI（系统包接口）总线互连，SPI 总线的带宽资源为 10G。

如图 2 所示，接入单元由 10G 光电信号转换模块，2.5G POS 光电信号转换模块 CP-3395 和成帧芯片 IXF19301 组成，10G 光电信号转换模块和 2.5G 转换模块不能同时使用，两种模块通过 SFI 接口和成帧芯片连接，成帧芯片通过高速 SPI-4.2 接口与主控单元连接；所述 10G 光电信号转换模块可兼容 10G POS（基于同步数位阶层光纤网络的数据包）、10G LAN（局域网）、WAN（广域网络）。

如图 3 所示，主控单元由网络处理器单元 NP-1322 和 4 路千兆物理接口 c8304 组成，网络处理器单元包括帧头信息处理模块、分类查找处理模块、转发决策处理模块；帧头信息处理模块通过 SPI-4.2 接口与接入单元相连，分类查找处理模块与帧头信息处理模块相连，转发决策处理模块与分类查找处理模块相连，转发决策处理模块通过 GMII（千兆位媒体独立接口）与安全审查单元相连，转发决策处理模块通过 XAUI（附件单元接口）与交换输出单元相连。主控单元是所述安全过滤分流器的核心处理单元，主要负责对接入单元接收并处理过的数据包进行粗过滤（通过预先设置粗粒度数据包内容检查规则）和数据分流策略的判定。主控单元采用网络处理器实现，由于网络处理器具有可编程的特性，因此可以根据实际应用的需要灵活选择适用的负载均衡算法。

如图 4 所示，安全审查单元由 4 个带千兆电口接口的标准 CPU 处理模块组成，所述 4 个 CPU 处理模块采用并行处理的工作模式，实现对数据包内容的细粒度检

查。虽然网络处理器与通用处理器相比在数据处理上具有明显的优势，但是网络处理器的优势主要在于网络层以下的包处理上，由于对数据包进行应用层的细粒度过滤具有一定的复杂性，若是采用网络处理器进行应用层的内容处理则会导致网络处理器性能的下降，因此安全审查单元采用通用 CPU 处理器实现。

如图 5 所示，交换输出单元主要由千兆交换主控模块、千兆电口接口模块、千兆光口接口模块组成，交换输出单元共 8 个千兆电口和 4 个千兆光口，千兆交换主控模块通过 GMII 接口分别与千兆电口接口模块和千兆光口接口模块相连，交换输出单元根据主控单元制定的分发策略完成数据转发操作。

本发明的主要工作流程如下：

由接入单元 1 对来自网络中的各种类型的数据流进行光电转换、串/并转换，帧处理，数据流按照 PPP/HDLC Over SONET/SDH 规范从 SONET/SDH 数据流还原为 PPP 数据包，然后通过高速接口传递给主控单元 2；

主控单元 2 按照标准协议规范检验接入单元发送过来的数据包的完整性，然后，按照预先设置的过滤规则对数据包进行七层线速过滤，过滤掉非法数据包和异常数据包；

主控单元 2 把需要进行深度内容检查的数据包提交给安全审查单元作进一步的细粒度的内容分析，对于不需要进行细粒度内容审查的数据包，有主控单元 2 根据负载均衡算法运算得出该数据包的分流策略，并将制定好的数据分流策略下发给交换输出单元 4 执行具体的数据转发操作；

安全审查单元 3 按照细粒度过滤规则对数据包的内容进行深入过滤，将过滤结果反馈给主控单元 2，主控单元 2 根据细粒度过滤结果为该数据包制定分流策略，并将制定好的数据分流策略下发给交换输出单元 4 执行具体的数据转发操作；

对局域网内的服务请求的转发处理，由交换输出单元 4 通过检验数据包头中“SYN”字段的值来判断该的数据包是否为新建立会话的第一个报文段，将新建立的会话的第一个数据包发送给主控单元 2 进行新会话的分流策略判定。主控单元 2 仅对每个会话的第一个数据包进行数据分流策略的判定，由交换输出单元 4 通过检验数据包结束标志“FIN”的值来判断当前的会话是否结束，对于属于同一个会话的后续数据包由交换输出单元 4 根据主控单元 2 制定并下发的数据分流策略执行具体的策略判断与数据转发处理操作。

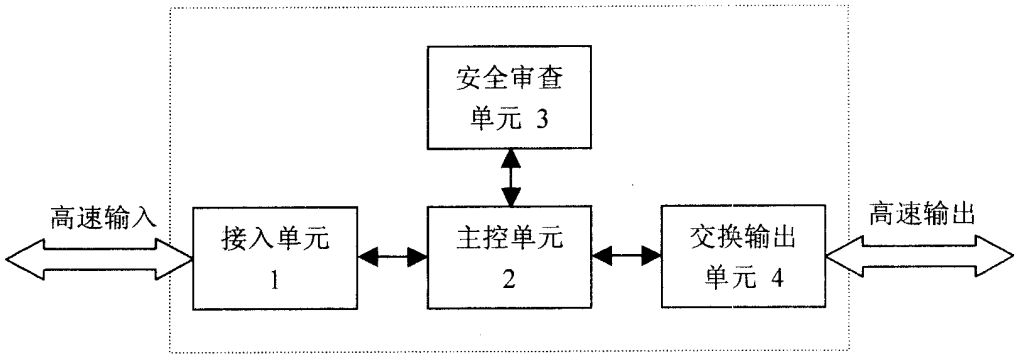

安全审查
单元 3
高速输入
接入单元
1
主控单元
2
交换输出
单元 4
高速输出

图 1

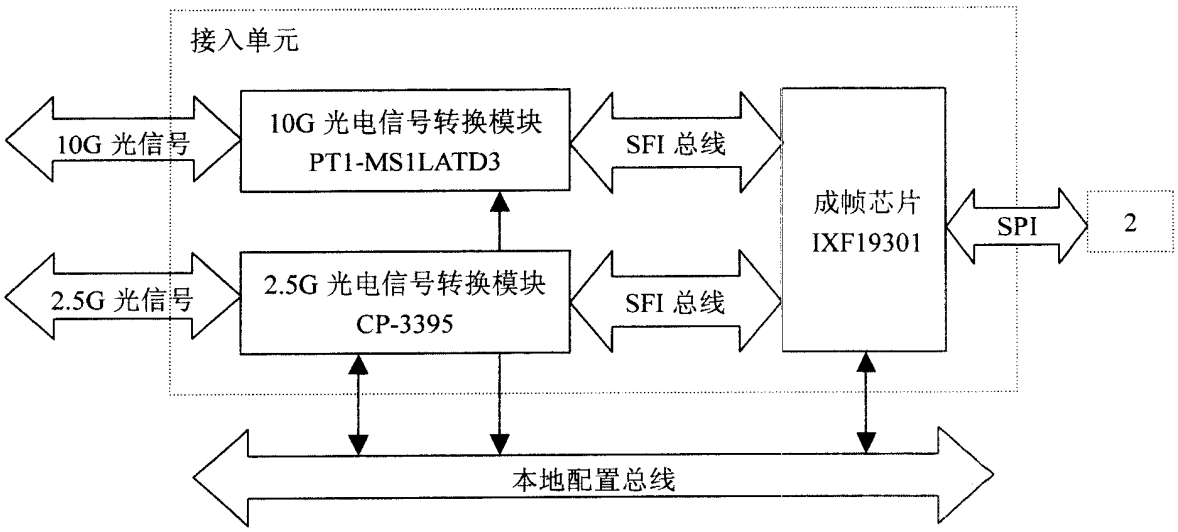

接入单元
10G 光信号
10G 光电信号转换模块
PT1-MS1LATD3
SFI 总线
成帧芯片
IXF19301
SPI
2
2.5G 光信号
2.5G 光电信号转换模块
CP-3395
SFI 总线
本地配置总线

图 2

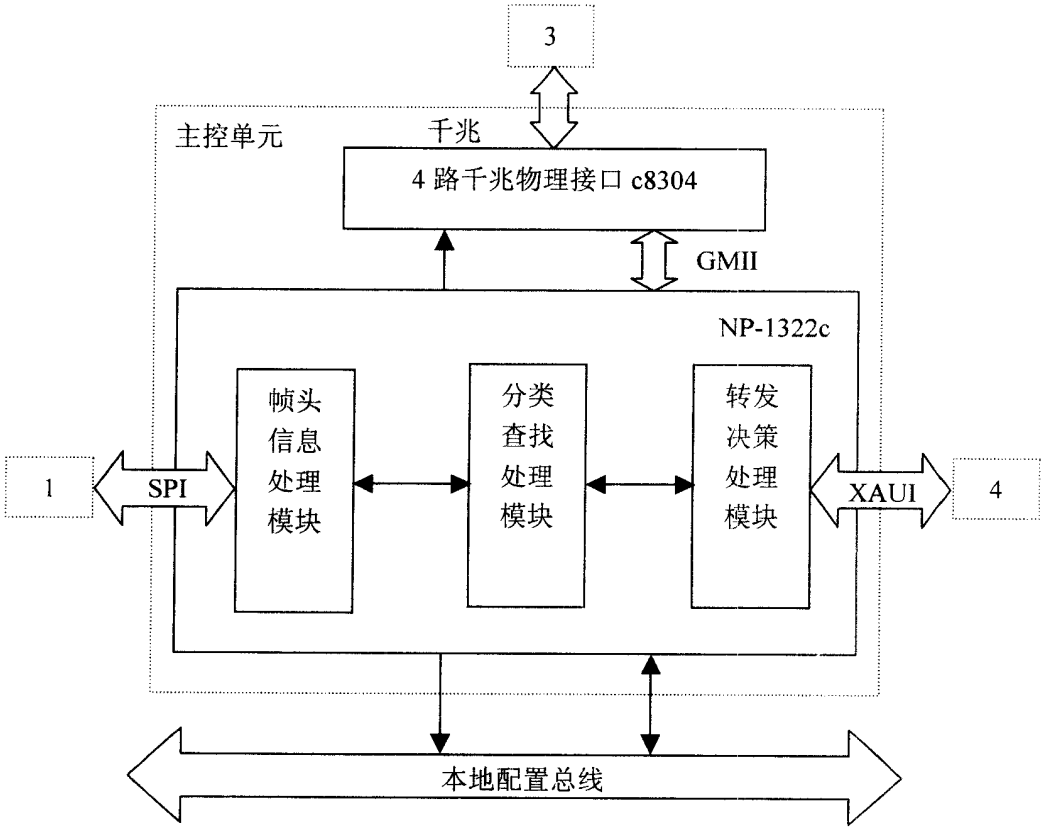

3
主控单元
千兆
4 路千兆物理接口 c8304
GMII
NP-1322c
帧头
信息
处理
模块
分类
查找
处理
模块
转发
决策
处理
模块
1
SPI
XAUI
4
本地配置总线

图 3

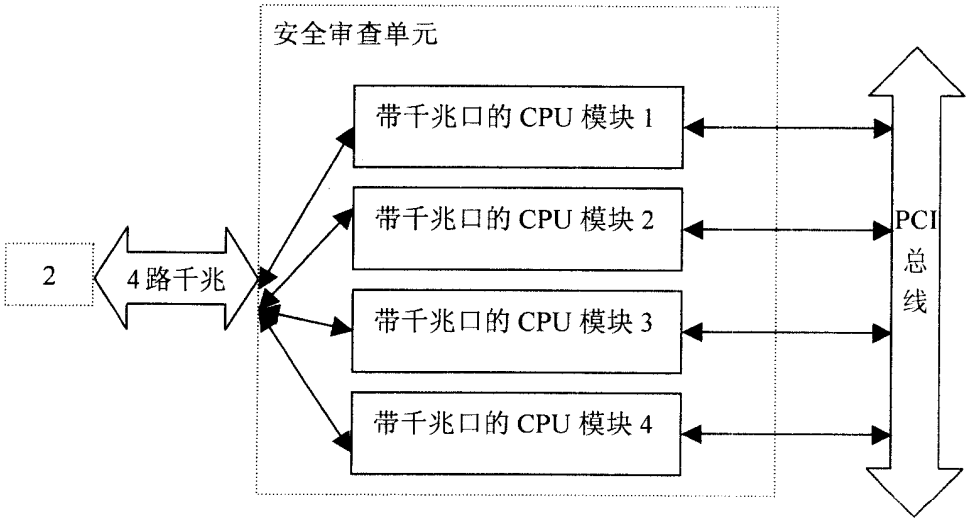

安全审查单元
带千兆口的 CPU 模块 1
带千兆口的 CPU 模块 2
带千兆口的 CPU 模块 3
带千兆口的 CPU 模块 4
2
4 路千兆
PCI
总
线

图 4

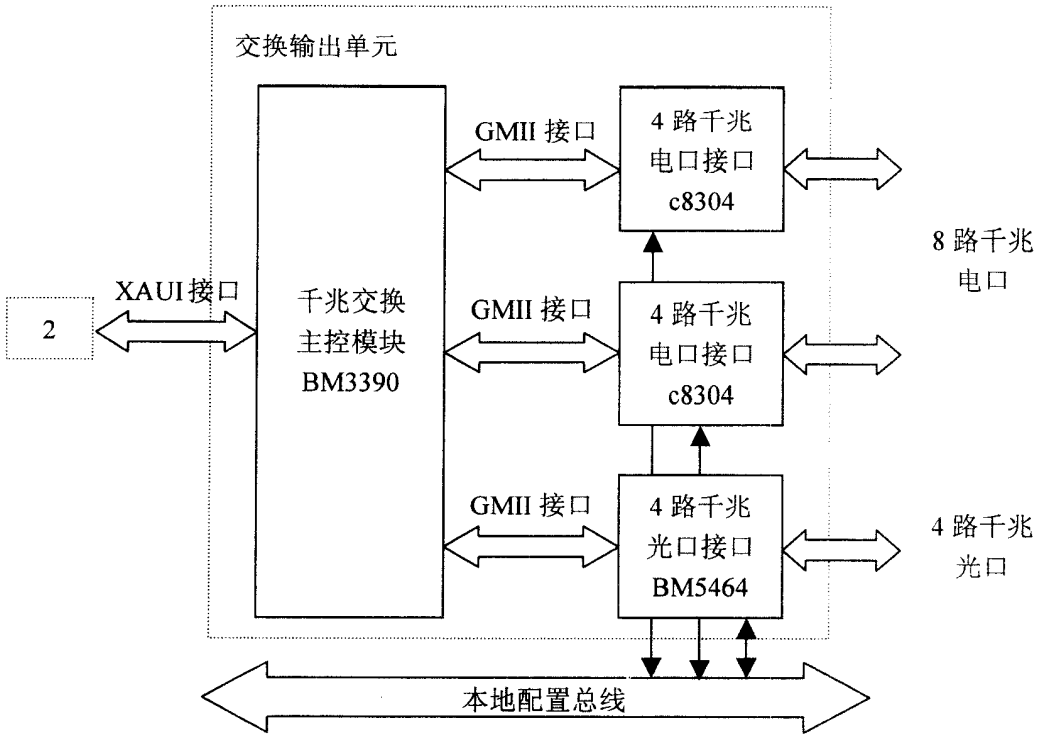

交换输出单元
千兆交换
主控模块
BM3390
GMII 接口
4 路千兆
电口接口
c8304
GMII 接口
4 路千兆
电口接口
c8304
GMII 接口
4 路千兆
光口接口
BM5464
XAUI接口
2
8 路千兆
电口
4 路千兆
光口
本地配置总线

图 5