计算机测量与控制.2014.22(6)
Computer Measurement & Control

文章编号:1671-4598(2014)06-1893-03　　中图分类号:TP206.1　　文献标识码:A

基于高速双端口的网络扫描系统研究

李求根，黄天波，王　颖
（中国电子科技集团公司 第五十研究所，上海　200331）

摘要：网络扫描是网络测试工作中一个非常重要的环节，为提高网络扫描速率和增强扫描功能，对双端口网络扫描系统进行了研究；该系统拟采用双端口线速数据流发送与接收相分离的方式，同时结合发送数据流字段变化、接收地址学习、接收规则过滤等技术，使其形成多种高速网络扫描功能；应用分析表明，扫描速率最高可达156万次/秒，且功能具备实用、灵活和多样化等特点。

关键词：端口扫描；主机扫描；双端口；数据流；线速

Research and Realization of Network Scanning System Based on Dual－port High－speed

Li Qiugen，Huang Tianbo，Wang Ying
（China Electronics Technology Group Corporation Fiftieth Institute，Shanghai　200331，China）

Abstract：Network Scanning is a vital part in Network testing. In order to improve the network scanning rate and enhance the network scanning function，the dual－port network scanning system is studied. The system realizes the separation between dual－port line speed data stream transmitting and receiving. At the same time，combining send data flow field change，receiving address learning，receive rules filtering and other technology，making the system develop a variety of high－speed network scanning feature. The application shows that the scanning rate up to 1560000 times per second，and possess the function of practical，flexible and diverse.

Key words：port scan；host scan；dual－port；data stream；line speed

0　引言

随着信息化网络建设的不断深入，人们的日常生活与工作对信息网络系统的依赖也越来越深。越来越多的关键数据储存在信息网络系统中，越来越多的核心业务通过信息网络系统来实现，越来越多的信息交换与数据传输也通过信息网络系统来实现。因此，对整个信息网络系统的功能正确性，执行效率，运行稳定性，可靠性，安全性提出了越来越高的要求。

在上述发展背景下，网络测试作为保障整个信息网络系统正常稳定运行的重要手段，起到了日益重要的作用。而无论是网络传输性能测试还是网络安全性能测试，网络扫描技术都是其中必不可少的一种技术手段和方法。面对越来越复杂的信息化网络系统，随之运行于单机上的扫描系统耗时也越来越多，占据了整个测试过程的大量时间，为改变当前的网络扫描方式，提高测试效率，本文研究和设计了一种高速双端口网络扫描系统。

1　网络扫描应用场景

网络扫描技术在应用过程中将面临多种不同的应用场景。常见有如下几种情况：

（1）对给定或指定IP段进行主机扫描；
（2）对给定或指定IP主机进行端口扫描；
（3）对给定或指定IP段进行MAC地址扫描；
（4）对未知网段进行主机扫描。

收稿日期：2013-12-26；　**修回日期**：2014-01-07。

作者简介：李求根(1984-)，男，江西人，工程师，工学硕士，主要从事网络测试技术、通信装备测试仪器开发技术等方向的研究。

2　网络扫描基本原理

2.1　主机扫描

主机扫描可利用ICMP数据报文实现，也是最简单最基本的探测手段，用来判断目标是否活动。主机扫描工作原理[1]：向目标发送一个要求回显的ICMP数据报文，当主机得到请求后，再返回一个回显数据报文，通过数据分析来确定这个网段的网络运作情况。

2.2　端口扫描

端口扫描是一种非常重要的探测手段，它是一种可以自动检测远程或本地主机安全性弱点的方法，可以不留痕迹地发现远程服务器的各种TCP端口的分配状态以及提供的服务和它们的软件版本，这样就能间接或直观地了解到远程主机所存在的安全问题[2]。端口扫描的工作原理[3]：向远程主机的端口发送不同的TCP标志包（TCP端口扫描），目标主机的端口状态（开放、关闭等）不同，对这些TCP标志包的回应包就有所不同，然后分析这些回应包，就可得出远程主机的端口开放情况。比如（是否能用匿名登陆，是否有可写的FTP目录，是否能用TELNET，HTTP）。发送的也可以是UDP包（UDP端口扫描），但UDP端口扫描简单，很容易被检测到，因此，目前使用最多的是TCP端口扫描。

2.3　MAC地址扫描

MAC地址扫描是一种基于ARP协议工作的扫描技术，主要是在确定IP地址但未知MAC地址时进行的扫描。MAC地址扫描工作原理[4]：当主机不知指定IP主机的MAC地址时，则向网络中广播MAC地址为“FF：FF：FF：FF：FF：FF”和目的IP为已知地址的ARP询问数据包，网络上其他主机并不响应该ARP询问，只有指定IP主机接收到数据包后

才向询问主机发送一个带有自身 MAC 地址的数据包，主机接收到响应数据包后通过解析即可获取指定 IP 地址主机的 MAC 地址。

3 双端口扫描系统设计

3.1 扫描系统总体结构设计

通过对主机扫描、端口扫描和 MAC 地址扫描的原理分析，确定该 3 种扫描方式分别基于 ICMP、TCP/UDP、ARP 等协议的数据报文发送和响应数据报文分析完成扫描工作。为提高网络扫描效率和准确率，本文避开普通网络适配器的性能瓶颈，设计了一个基于高速 FPGA 的双端口扫描系统，将数据流的产生工作和接收工作均由 FPGA 实现，但分别应用不同的端口。其总体结构如图 1 所示，用户在主控系统中通过应用软件配置扫描参数，然后通过总线下发到扫描单元，由命令解析模块将接收到的下行数据进行解析并配置发送模块，发送模块向端口 A 以线速发送符合要求的数据流；当数据流到达目标主机时，其产生的响应数据流将传输流向端口 B，接收模块将根据要求进行匹配过滤，数据解析模块从过滤接收的数据流中提取特征数据发向主控系统，主控系统接收到上行数据分析后进行结果显示。

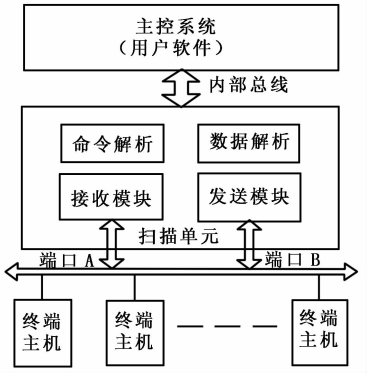

图 1 双端口扫描系统总体结构

3.2 线速数据流发送模块设计

线速数据流发送模块是扫描系统的核心模块之一，其负责以线速将设置完成的数据流发向网络系统或被测设备。数据流[5]是实时的、连续的、有序的、具有一定特征的序列，它具有如下特点：有序性、实时性、连续性、无限性、单遍性、概要性、低层次性、多维性、近似性、及时性。因此，本模块根据上面所述的主机扫描、端口扫描和 MAC 地址扫描需求，确定了数据流的特征字段为目的 MAC 地址、源 MAC 地址、帧类型、协议类型、源 IP 地址、目的 IP 地址、源端口、目的端口及 TCP 连接标志位等 9 个字段，每个字段均可独立以固定、步进递增、步进递减、指定及随机等 5 种方式进行变化。例如，当设置源端口以步进为“2”的递增方式，而其他字段设为固定方式时，本模块将发送其他字段不变而源端口以步进为“2”逐一变化的数据流。

为实现以上功能，发送模块功能设计如图 2 所示，主要由控制管理模块、字段处理模块、校验模块和 MAC 模块组成，其中控制管理模块接收控制信号判别发送数据流类型及其字段变化要求，组织数据流构成和校验和计算，由字段处理模块最终构成数据流发送到 MAC 模块，经由 MAC 模块处理后直接发送到 PHY 层，通过网络接口传输到网络中。

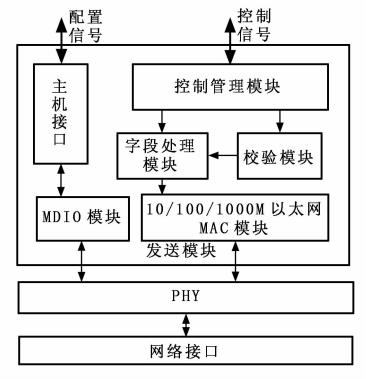

图 2 线速发送模块功能框图

3.3 接收匹配过滤模块设计

接收匹配过滤模块主要完成数据流的接收，并按照一定特征字段进行匹配，实现数据流过滤接收。它与发送模块配合协同工作，是扫描系统的重要功能模块。同理，该模块具有目的 MAC 地址、源 MAC 地址、帧类型、协议类型、源 IP 地址、目的 IP 地址、源端口、目的端口及 TCP 连接标志位等 9 个匹配字段，可将符合字段的数据流接收并处理，不符合字段的数据流进行丢弃。为增加匹配字段应用的多样性和灵活性，设计了“与”、“或”和“非”等 3 种匹配规则，“与”规则表示该字段必须符合，否则丢弃；“或”规则表示只要符合该字段即可接收；“非”规则表示接收不符合该字段的数据流，符合该字段的则进行丢弃。应用示例如下，当设置匹配规则为：目的 MAC 地址（AND）、源 MAC 地址（AND）、帧类型（AND）、协议类型（AND）、源 IP 地址（AND）、目的 IP 地址（AND）、源端口（AND）、目的端口（||）、TCP 连接标志位（NOT），则表明可以接收不满足 TCP 连接标志位，但同时满足目的 MAC 地址、源 MAC 地址、帧类型、协议类型、源 IP 地址、目的 IP 地址的数据流或者满足目的端口的数据流，否则予以丢弃。

根据以上接收匹配需求，接收匹配过滤模块功能设计如图 3 所示，其主要由字段规则模块、字段提取模块和 MAC 模块组成。MAC 模块将接收到的数据流发送给字段规则匹配模块，字段规则匹配模块将根据预先设置的字段和规则对数据流进行比较分析，符合字段匹配规则的数据流则发送到字段提取模块，不符合的则进行丢弃。字段提取模块将过滤接收的数据流进行相应字段提取并反馈到主控系统，从而完成数据流的接收匹配过滤工作。

3.4 终端应用软件设计

终端应用软件用于用户与扫描系统之间的交互，主要完成参数设置、测试数据组织和结果显示三大任务。其具备扫描方式选择功能、测试数据流配置和组织功能、匹配规则设置功能和结果显示功能。该软件运行于主控系统中，具体设计框图如图 4 所示。

4 场景应用分析

基于以上扫描原理分析和设计实现，现进行扫描系统应用分析，由于篇幅原因，在此只分析主机扫描方式，其他同理，测试连接如图 5 所示。

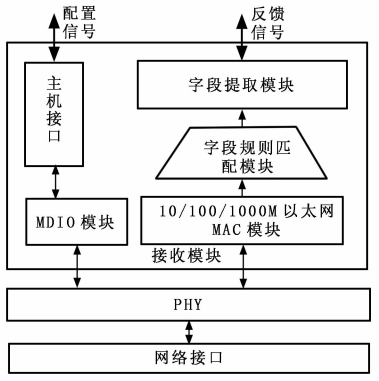

图 3　接收匹配过滤模块功能框图

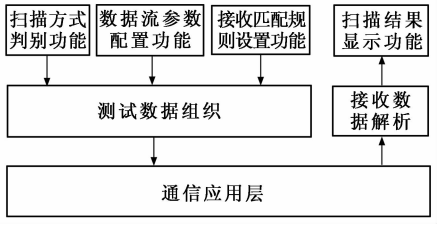

图 4　终端应用软件组织框图

当对给定或指定 IP 段进行主机扫描时，测试数据流目标 IP 字段变化字节初始值设为 1，变化方式设为递增，步进设为 1；其他字段设置初始值（协议值设为 ICMP），且变化方式设为固定。匹配字段和规则设置如下：目的 MAC 地址字段设为与测试流源 MAC 一致，规则设为 AND；协议字段设为 ICMP，规则设为 AND；其他可忽略。测试发起前，接收端口 B 应先对交换机进行地址学习，发送端口 A 再进行测试流发送，当测试流遇到与其 IP 字段一致的活动主机时，该主机将回应相应的数据流，并被传输至接收端口 B，接收模块匹配后进行源 IP 字段提取，反馈给主控系统进行显示。

当对未知网段进行主机扫描时，需要对全网段进行扫描，设置同上。最糟糕的情况需进行 2^{32} 次测试流发送，在此以 1 000 Mbps 的线速进行发送，IPG 设为 8 字节，帧长设为 64 字节，则 1 s 大约可发送 1.56×10^6 帧，因此发送 2^{32} 帧需耗时约 45 min，可见扫描效率是非常高的。

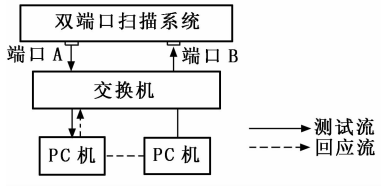

图 5　应用连接图

5　结束语

本文在分析扫描原理的基础上，针对各种应用场景提出了一种新的扫描系统，并详细阐述了各部分的设计思路。研究表明，该扫描系统具有如下特点：(1) 扫描效率高，远远高于常用扫描软件或系统的扫描效率；(2) 扫描效果好，基于高扫描效率，可根据情况实现重复扫描，大大降低漏扫率；(3) 应用灵活，可根据需求配置实现更多的扫描方法。基于该种扫描系统，经过后续研究还可以开发出更多的扫描应用，如漏洞扫描、密码扫描、服务扫描和系统扫描等。因此，该扫描系统设计方法具有一定的实用性和推广价值。

参考文献：

[1] 洪　宏，张玉清，胡子濮，等. 网络安全扫描技术研究 [J]. 计算机工程，2004，30 (10)：54－56.

[2] 李继容，曾爱国. 一种改进的端口扫描器的设计与实现 [J]. 计算机测量与控制，2010，18 (7)：1664－1666，1679.

[3] 张登银，许芳颂. 端口扫描与反扫描技术研究 [J]. 南京邮电学院学报. 2005，25 (6)：54－58.

[4] 曾光裕，薛莹莹，徐　冰，李清宝. 基于 ARP 协议的网络监听技术研究 [J]. 计算机工程与设计，2009，30 (14)：3269－3271.

[5] 罗　莎，朱　威，王培源，等. 网络数据流分析方法 [J]. 大地测量与地球动力学，2011，31 (s)：146－148.

[6] 柳利军，熊良芳. 基于 FPGA 的千兆以太网交换芯片的设计 [J]. 微电子学与计算机，2006，23 (3)：80－82，84.

(上接第 1892 页)

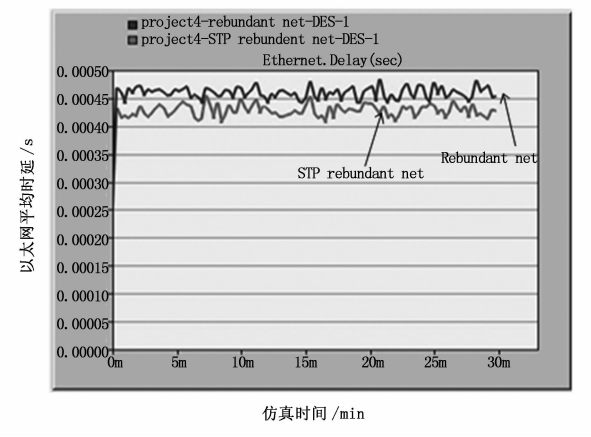

图 5　以太网时延对比图

4　结论

本文把生成树冗余和 VLAN 技术应用在基于以太网的列车通信网络中，有效地保证了通信网络的可靠性和稳定性，为消除环网广播风暴提供了有效途径，同时数据在 VLAN 中广播通讯不会占用更多的带宽，减少了数据的冲突机率。为了该通信网络实现生成树冗余和划分 VLAN，本文设计并制作了基于 KSZ8995MA 的交换机，经过测试，本交换机完全符合设计要求，已经成功地运用于基于以太网的列车通信网络。本文对其他同类网络的设计具有极大参考价值。

参考文献：

[1] 苗　剑，贺德强，丁超义. 基于工业以太网的列车通信网络及其仿真研究 [J]. 计算机测量与控制，2010，18 (10)：2417－2420.

[2] 姜立群，徐皑冬，宋　岩，等. 基于以太网现场总线冗余技术研究 [J]. 仪器仪表学报，2008，29 (4)：712－715.

[3] Zhang Q Z，Zhang W D. Network partition for switched industrial Ethernet using genetic algorithm [J]. Engineering Applications of Artificial Intelligence，2007，(20)：79－88.

[4] 马素刚. VLAN 技术的研究与仿真 [J]. 制造业自动化，2011，11 (33)：78－80.

[5] 牛占平. VLAN 技术在智能化变电站网络中的应用探讨 [J]. 电力系统保护与控制，2009，37 (23)：75－78.