基于 FPGA 的网络协议分析仪设计

王　瑞
（重庆城市职业学院，重庆 永川，402160）

摘要：随着网络技术的发展，网络在现代生活中越发重要，物联网技术的广泛应用使万物互联成为可能，这也对网络通信链路的性能提出了更高的要求。通信链路需要具备稳定性、健壮性、可测试性等特点，同时也需要配套的协议分析仪来监测与维护，这需要新兴的、应用方便的协议分析仪来保障链路质量、测试网络设备，进而支持网络底层协议的开发。

本文介绍的系统是在 FPGA 端作数据接收和处理、在 ARM 端作数据显示的处理速度达到千兆级别的简易网络协议分析仪，经测试，最大可分析流量达到千兆，不同协议的流量统计较为准确，FPGA 的最大延迟在 0.02ms 左右。

关键词：FPGA；千兆；网络协议分析

随着互联网的不断发展，万物互联成为社会的前进方向，网络已经成为人们生活和工作中不可或缺的部分，随着网络规模的不断扩大，通信链路变得越来越复杂，数据流量也快速增长，这使得网络故障出现的概率提高。目前业界将主要精力放在了物联网的应用开发、商业模式等方面，对于物联网安全却疏于考虑，使得物联网安全现状令人堪忧。这些都对网络通信链路的性能提出了更高的要求，通信链路需要具备稳定性、健壮性、可测试性等特点，同时也需要配套的协议分析仪来检测与维护。

网络协议分析仪是一种用于监测、分析网络流量的工具，它的研发和应用具有多方面的意义：

（1）诊断网络故障。网络协议分析仪可以对网络数据流进行数据处理，可以实时监测到异常的流量情况，从而帮助诊断网络故障。

（2）优化网络设计。网络协议分析仪可以帮助分析网络带宽的占用情况，用户根据分析结果可以调整网络拓扑结构、优化带宽分配等，提高网络效率和可靠性。

（3）提升网络安全性。不同类型的网络攻击在流量、包特征上有明显区别，网络协议分析仪可以实时检查这些特征，并提供实时警报和日志记录，这可以帮助用户及时发现并应对安全威胁，保障网络的安全性。

本文将设计一套基于 FPGA 的网络协议分析方案，该系统可以接入网络的镜像源或直接工作于网络中，像滤网一样筛查通过本段网口的报文，并对当前的网络报文流量进行实时统计分析，并实时显示结果。

一、系统方案设计

（一）系统整体方案

本系统以 Artix-7 系列的 FPGA 芯片作为核心处理器，并选择 stm32h743 作为 ARM 部分的处理器。分析仪通过千兆网口接入网络，在触摸屏对统计内容进行控制。网络报文的物理信号在网口被接收后，由 PHY 芯片将物理层信号转为数据链路层的数据帧，再由 FPGA 芯片通过 RGMII 协议与 PHY 芯片进行通信，将数据帧传输至网络协议实现模块，并对其进行数据处理与统计。最后将结果传输到屏幕上。此外用户可通过点击触摸屏，让 ARM 向 FPGA 发出控制信号，调整 FPGA 的数据统计功能。整体的系统框架如图 1 所示。

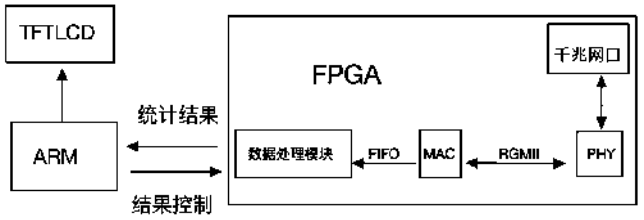

图 1 系统框架图

（二）ARM 与 FPGA 的通信方案

FPGA 与 ARM 之间的通信规则采用四相握手的协议，具体过程如图 2 所示。

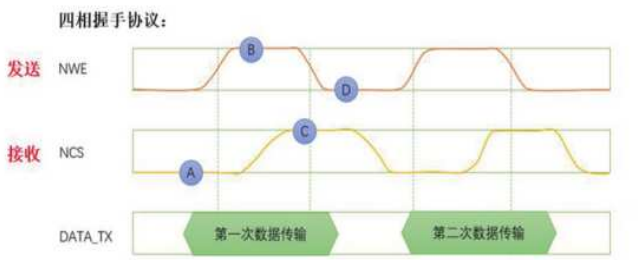

图 2 四相握手协议

NWE 为请求发送的信号线，NCS 为接收的信号线，DATA_TX 为双方进行数据传输的数据线。当双方不处于通信状态时，NWE 信号线和 NCS 信号线都处于低电平状态，同时时刻监测 NWE 信号线的状态；当任意一方需要向另一方发送数据时，发送方先将 NWE 信号线置为高电平，并将 DATA_TX 置为要传输的数据，并开始监测 NCS 信号线。接收方在监测到 NWE 信号线置为高电平后，将 DATA_TX 上的数据接收，并将 NCS 信号线置为高电平，示意已经完成接收。发送方在监测到 NCS 的抬起后将 NWE 置回低电平状态，接收方在监测到 NWE 信号线低电平后，将 NCS 信号线置回低电平状态，至此完成一次数据传输。

（三）核心处理器选择

本系统的核心处理器采用了 Artix-7 系列的 FPGA 芯片，该芯片型号为 xc7a35tfgg484-2。作为 Xilinx 的一块较为基础、结构简单的 FPGA 芯片，xc7a35tfgg484-2 能够实现大部分 FPGA 的功能，并且具有很好的移植性。在本系统中，该芯片负责网络报文的接收与处理。通过 FPGA 的灵活性和可编程性，本系统可以适应不同的网络环境和应用场景。

除了 FPGA 芯片之外，本系统还采用了 stm32h743 作为 ARM 部分的处理器。stm32h743 是一款高性能、低功耗的微控制器，拥有强大的计算能力和丰富的外设资源。在本系统中，stm32h743 主要用于处理用户的通过触摸屏对统计功能的调节，并向用户实时显示统计结果，实现与用户的交互。通过 FPGA 和 ARM 的协同作用，本系统可以实现高效、灵活、可靠的网络通信和用户交互。本系统的硬件框图如图 3 所示。

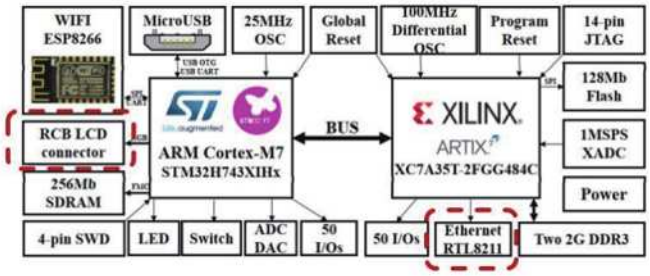

图 3 开发板资源布局

二、逻辑模块设计

（一）数据处理模块

数据处理模块的总功能是完成对 ARP、RARP、IP、ICMP、IGMP、TCP、UDP 报文流量的统计，因此如果做流量汇总，可以分两步进行，先通过以太网帧的第 13、14 字节判断 ARP、RARP、IP 的类型，若为 0x0806 则为 ARP 协议，若为 0x8035 则为 RARP 协议，这两种情况下就可以从 FIFO 中取出下一个报文进行分析。若为 0x0800 则为 IP 协议的报文，需要进一步分析是 IP 协议中的哪一种，在第 24 字节即 IP 协议的首部的协议段可以识别，若为 1 则为 ICMP 协议，若为 2 则为 IGMP 协议，若为 6 则为 TCP 协议，若为 17 则为 UDP 协议。

如果本系统考虑作用在镜像源工作，那么数据处理模块接收部分报文，在对首部完成解析后即可接收新的报文，但如果还要应用于网络通信的环境中，起一个类似于滤网的作用，那么数据处理模块就不能如此简单的处理报文，因为还要将报文重新转运送出，因此妥善的做法是新增一个深度为 1500 字节的 FIFO，因为一个以太网帧的最大长度是 1500 字节，在这个 FIFO 中完成识别功能，再将处理完的报文送入 TX_AXIS_FIFO 中，完成报文的传出。

（二）通信模块

通信模块指的是 FPGA 端通过 BUS 线向 ARM 提供统计数据的模块，FPGA 端主要完成的工作是每间隔 1s 主动置高 NWE 信号线，并实时监听 NCS 信号线，当接收线也被置为高电平时，依次传出 ARP 流量、RARP 流量、IP 流量、ICMP 流量、IGMP 流量、TCP 流量、UDP 流量和其他协议的流量，之后将 NWE 信号线置为低电平，并在 NCS 信号线置低后回到初始状态。为了防止通信过程影响了统计过程，使用一级缓存设计，在 1s 时将各流量数据存入新的 reg 中，旧的 reg 清零并立刻开始新的一轮计数，传出的流量数据事实上是新的 reg 中的数据。

尽管当前使用到的通信模式是单向的，但为了更好的功能拓展性，四相握手协议的全部内容都完成了搭建，即 FPGA 也在一直监听 NWE 信号线，若 NWE 信号线被置为高电平，则 FPGA 会置高 NCS 信号线，并将此时数据线上的电平输入到 FIFO 中，之后在监听到 NWE 信号线置为低电平后，将 NCS 信号线置为低电平。

三、系统测试与性能评估

（一）报文接收与发送能力测试

通过两台笔记本，其中一台作为报文发送端，另一台作为报文接收端，在网线直接连接情况下报文可以正常接收，除了测试报文接收、发送功能的完整性，还要测试整个过程的延时，如果处理过程消耗时间过长，显然是不可接受的。延时测试的初步方案是先由笔记本 A 去多次 ping 笔记本 B，通过抓包软件查看笔记本 B 的反应时间 4。除此之外，由于延时是可以明确计算出的，因为报文在 FPGA 内总是处于流通状态，通过 ila 核去查看报文在 FPGA 中传输的时序即可估算出延时的大小。

（二）统计功能正确性测试结果

在测试中笔记本 A 先向笔记本 B 以 1s 为间隔发送任意字符串，报文发送的协议是 UDP，发送端情况如图 4。此外网络初始连接时会有一部分 ARP 的报文，而在这个简单的局域网内由于没有交换机或路由器，ICMP 和 IGMP 协议的报文并不会出现，接收端情况如图 5 所示。这种流量不大的情况下，wireshark 软件记录的流量数据和显示屏上显示的流量数据一致。再测试大流量传输时统计功能是否准确，笔记本 A 向笔记本 B 传输一个 2.2Gb 的视频文件，在 10s 内传输完毕，此时 wireshark 软件记录的流量数据已经几乎全为 UDP 协议，总流量峰值为 840Mbps，这些结果也与触摸屏显示界面的流量数据保持一致。

图 4 发送端情况

30 14.097085	LCFCHeFe_d4:c5:6b	LCFCHeFe_0b:a2:90	ARP	60	Who has 192.168.1.2? Tell 192.168.1.3
31 14.097097	LCFCHeFe_0b:a2:90	LCFCHeFe_d4:c5:6b	ARP	42	192.168.1.2 is at 98:fa:9b:0b:a2:90
32 14.231980	192.168.1.2	192.168.1.255	UDP	305	54915 → 54915 Len=263
33 14.237619	192.168.1.3	192.168.1.2	UDP	60	8080 → 8080 Len=7
34 15.232632	192.168.1.2	192.168.1.255	UDP	305	54915 → 54915 Len=263
35 15.245902	192.168.1.3	192.168.1.2	UDP	60	8080 → 8080 Len=7
36 16.231644	192.168.1.2	192.168.1.255	UDP	305	54915 → 54915 Len=263
37 16.263191	192.168.1.3	192.168.1.2	UDP	60	8080 → 8080 Len=7
38 17.233855	192.168.1.2	192.168.1.255	UDP	305	54915 → 54915 Len=263
39 17.286859	192.168.1.3	192.168.1.2	UDP	60	8080 → 8080 Len=7
40 18.225534	192.168.1.2	192.168.1.255	UDP	305	54915 → 54915 Len=263
41 18.311618	192.168.1.3	192.168.1.2	UDP	60	8080 → 8080 Len=7
42 19.226404	192.168.1.2	192.168.1.255	UDP	305	54915 → 54915 Len=263
43 19.323289	192.168.1.3	192.168.1.2	UDP	60	8080 → 8080 Len=7

图 5 接送端情况

四、结语

本文设计完成了基于 FPGA 的以太网网络协议分析仪，在 FPGA 上完成报文接收、统计再传出的功能，并将统计结果显示在触摸屏上。该设计的吞吐流量上限为 1000Mbps，最大处理延迟为 0.02ms，可以正确的反映当前网络环境的总流量、网络层各协议的流量以及传输层各协议的流量，并且不会影响以太网正常通信。相比传统的通过软件进行协议分析，本设计完全基于硬件，摆脱了操作系统的约束，从底层对网络协议进行直接分析，结果更加真实可靠，且处理速度快、延时低。

参考文献：

[1] 陈悦 . 基于 RFC2544 的网络性能测试仪 [D]. 南京理工大学，2018.