THE UNIVERSITY OF QUEENSLAND

AUSTRALIA

FPGA Web Interface and Ethernet Network Controller using the RISC-V Processor

Project Proposal

Matthew Gilpin

45801600

Semester 1, 2023

The University of Queensland

School of Information Technology and Electrical Engineering

List of Abbreviations

Abbreviations	
IoT	Internet of Things
FPGA	Field Programmable Gate Array
pf	Packet Filter
MAC	Medium Access Control
ISA	Instruction Set Architecture

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter provides the necessary background and reasoning behind the proposed project.

1.1 Topic

In a technology age of growing numbers of cyber attacks and growing number of Internet-of-Things (IoT) devices being interconnected, it's paramount to ensure these devices operate safetly and securely. There are a plethora of different ways to reduce the likelyhood of cyber attacks. A common approach is to employ a firewall to filter out potentially malicious packets.

This project focuses primarily on securing edge IoT Ethernet networks.

1.2 Aims

The aims of the proposed FPGA Ethernet controller and web interface on a RISC-V processor are:

- Create a Custom MAC
- Create a Custom hardware based packet filter
- Use a RISC-V Softcore processor to control the packet filter and host a web interface

1.3 Custom MAC

The decision in creating a custom MAC might be considered as insteresting given the range of pre-existing Intellectual Property (IP) cores for Ethernet on FPGAs. The issue with the pre-existing solutions only have a single output to connect to something like a softcore processor. To create a firewall, the network traffic would need to pass through the processor. To decrease latency, a second interface can be added to the MAC to allow traffic to flow through a hardware-based firewall. This is analogous to the direct memory access (DMA) controller on most modern microprocessors.

1.4 Packet Filter Firewall

Usually, the first line of defence against bad actors, it is a vital component in a computer network and can become vastly complex. There are several types of Firewalls such as packet filters (pf), stateful packet firewalls and application firewalls [1]. Firewalls can also perform other tasks and employ other techniques to secure a network, however, in this project the most basic pf-style firewall will be implemented. Packet filters are considered as stateless and traditionally only filter on the fields in the headers in the network (layer 2) and transport (layer 3) layers [1]. Such fields include IP addresses, port numbers and protocol type.

More advanced firewalls can perform deep packet inspection and explore the contents of the higher layers to better evaluate a packets true intention. While there is provision to add this functionality on an FPGA based firewall, this will not be explored in this project due to its significant increase in complexity.

1.5 RISC-V processor

Chapter 2

Background

Introduce the broad layout of the chapter.

2.1 Introduction

The IEEE 802.3 standard [2], more commonly known by the name of 'Ethernet' defines the *'Medium Access Control'* (MAC) protocol amongst other things for two or more devices to communicate over a network. This standard is just one part in the layered network models such as the OSI model and TCP/IP models.

RISC-V, a reduced instruction set computer architecture, is an open and royalty free instruction set architecture (ISA). As a result, a plethora of soft-core processors have been made. The specific core proposed in this project is the 'NEORV32' RISC-V processor. It's a highly configurable microcontroller like system on chip (SoC) written purely in VHDL.

Chapter 3

Timeline and Plan

This section of the report details the plan and timeline of the proposed project. It also details the necessary risk assessment.

3.1 Milestones

Table 3.2 shows the tasks and expected durations of the proposed project.

Task	Details	Duration
Create MAC	Create custom Layer 2 Ethernet hardware based on the IEEE 802.3 standard	3-4 Weeks
Wishbone Interface	Connect the Ethernet MAC to the NEORV32 RISC-V Processor using the wishbone interface and access it via software	2 Weels
Webserver	Create and Get the webserver working on the NEORV32 Processor. Web page should be accessed from another computer	5-6 Weeks
Firewall Hardware	Create the hardware between 2 Ethernet MACs to filter out packets based on rules	3-4 Weeks
Integration with software	Add functionality to the server to be able to configure the firewall rules	1 Week
Measure and Compare	Compare to pre-existing solutions	1 Week

Table 3.1: Milestones for the proposed project

3.2 Project Risk Assessment

The majority of the work compeleted in the proposed project is digital and poses little risk outside of the standard office sitting.

Risk	Severity	Likelyhood	Mitigation
Licensing	Minor	Moderate	Avoid software/hardware that requires a specific license.
Data loss	Catastrophic	Unlikely	Ensure all items are backed-up to the cloud and use services such as GitHub where appropriate. Employ a 3 2 1 backup strategy
Hardware Failure	Moderate	Unlikely	Double check all connections to the FPGA board before powering. Reduce excessive handling where necessary to minimise risk of damaging the equiptment
Illness	High	Likely	Take breaks periodically to avoid being over-worked, and take necessary recovery steps if sick.
Missed Deadlines	Major	Likely	Ensure plans are followed and compelete tasks as soon as possible. If behind, spend extra time on project to catch up.

Table 3.2: Risk assessment of proposed project

Chapter 4

Conclusion

Conclude your thesis.

Bibliography

[1] E. W. Fulp, "Chapter e74 - firewalls," in *Computer and Information Security Handbook*, pp. e219–e237, Elsevier Inc, third edition ed., 2017.

[2] "IEEE Standard for Ethernet," standard, The Institute of Electrical and Electronics Engineers, Inc., New York, USA, Dec. 2012.

Appendix A

Appendix

Write your appendix here. Following two are examples.

A.1 Name of Appendix-1

A.2 Name of Appendix-2