THE UNIVERSITY OF QUEENSLAND

AUSTRALIA

# Wire-speed FPGA packet filter with Ethernet MAC and web server using a RISC-V softcore 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 Abbreviations** **ii**

**Contents** **iii**

**List of Figures** **iv**

**List of Tables** **iv**

**1 Introduction** **1**

1.1 Background . . . . . . . . . . 1

1.2 Topic . . . . . . . . . . 1

1.3 Defining IoT edge netwoks . . . . . . . . . . 1

1.4 Aims . . . . . . . . . . 1

1.5 Establishing Exclusions . . . . . . . . . . 2

**2 Abbreviated title** **3**

2.1 Introduction . . . . . . . . . . 3

2.2 Custom MAC . . . . . . . . . . 3

2.3 Packet Filter Firewall . . . . . . . . . . 3

2.4 RISC-V processor . . . . . . . . . . 4

**3 Abbreviated title** **5**

3.1 Milestones . . . . . . . . . . 5

3.2 Project Risk Assessment . . . . . . . . . . 5

**4 Conclusion** **7**

**Bibliography** **8**

**A Appendix** **9**

A.1 Name of Appendix-1 . . . . . . . . . . 9

A.2 Name of Appendix-2 . . . . . . . . . . 9

# List of Figures

# List of Tables

3.1 Milestones for the proposed project . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
3.2 Risk assessment of proposed project . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

Chapter 1

# Introduction

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

## 1.1 Background

In a technology age of growing numbers of cyber attacks and record number of connected devices, it's paramount to ensure these devices operate safetly and securely. In the 2021-22 financial year the Australian Cyber Security Center (ACSC) recieved in excess of 76,000 cybercrime reports and growing [1].

## 1.2 Topic

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.

## 1.3 Defining IoT edge netwoks

## 1.4 Aims

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

- Increase security to edge IoT networks.
- Increase the power efficiency for wire-speed firewalls.

## 1.5 Establishing Exclusions

While the proposed project will reduce the likelyhood of network based attacks it is not a *'one size fits all'* solution. By the nature of the IoT and edge network ecosystem, there are a myriad of different attack vectors where not all of them will be detectable at the netowrk level.

The proposed project will **not**

- Protect against all attacks
- Be able to protect against all IoT devices.
- Not perform routing

# Chapter 2

# Background

Introduce the broad layout of the chapter.

## 2.1 Introduction

## 2.2 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.

## 2.3 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 [2]. 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 [2]. 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.

## 2.4 RISC-V processor

The IEEE 802.3 standard [3], 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 overworked, 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] A. C. S. Center, “Acsc annual cyber threat report, july 2021 to june 2022,” Nov 2022.

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

[3] “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